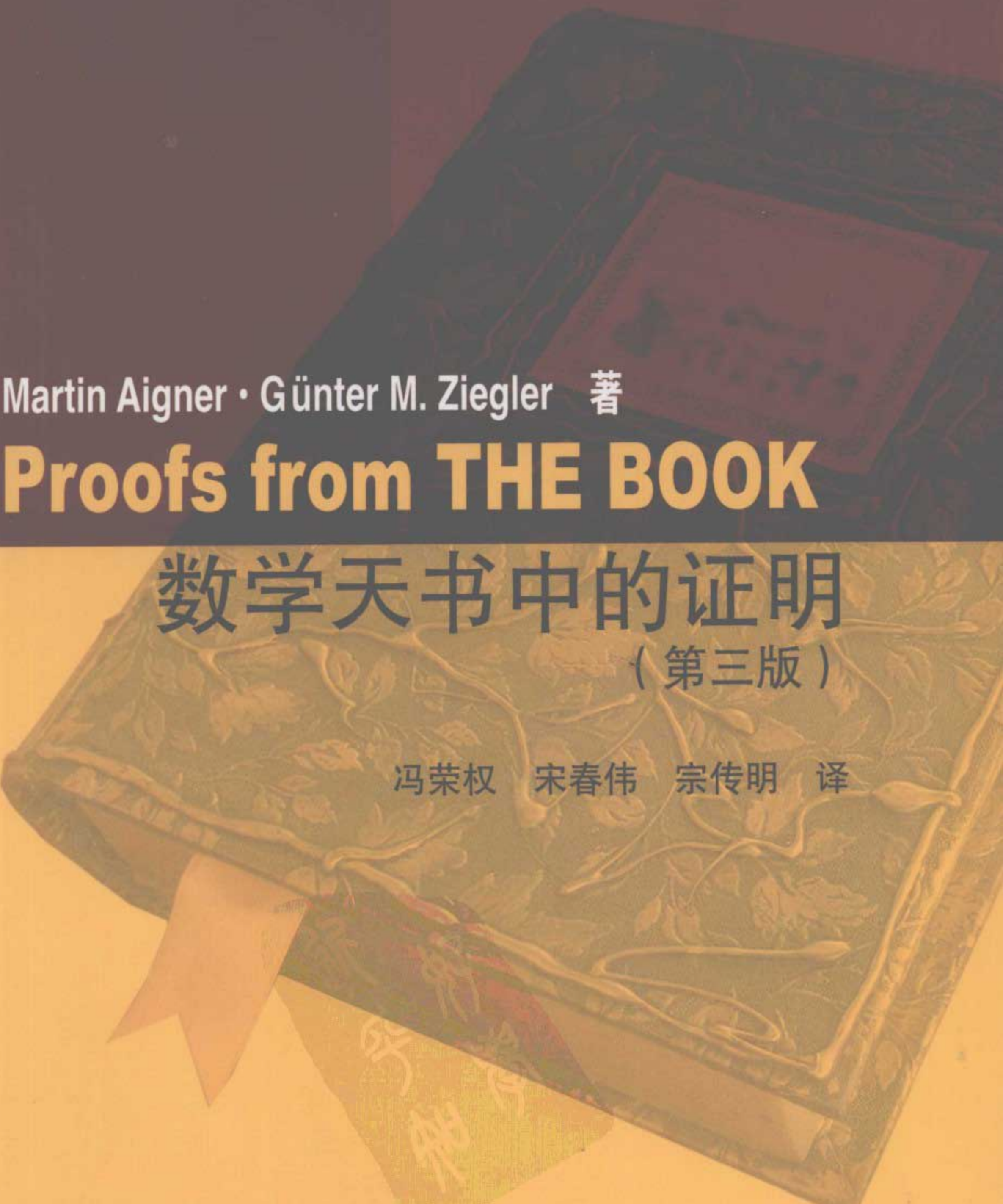
Martin Aigner · Günter M. Ziegler 著

Proofs from THE BOOK

数学天书中的证明

（第三版）

冯荣权 宋春伟 宗传明 译



高等教育出版社
HIGHER EDUCATION PRESS

本书介绍了35个著名数学问题的极富创造性和独具匠心的证明。其中有些证明不仅想法奇特、构思精巧，作为一个整体更是天衣无缝。难怪，西方有些虔诚的数学家将这类杰作比喻为上帝的创造。这不是一本教科书，也不是一本专著，而是一本开阔数学视野和提高数学修养的著作。希望每一个数学爱好者都会喜欢这本书，并且从中学到许多东西。

本书的英文原著第一版于1998年出版。随即受到数学界的广泛好评，并被陆续翻译成了十余种不同的文字，其中包括法文、德文、意大利文、日文、西班牙文和俄文等。

“本书中的内容确可谓之数学天堂一个缩影，人们敏锐的洞察力、绚烂的思想是如此巧妙地融入其中。字里行间蕴含着巨大的财富，人类思想的珍宝源源不断地涌现。一些证明是经典的，但更多经典结果都有了极具智慧的新证明。 … Aigner和Ziegler …写道：‘我们精心挑选了这些例子，目的是希望读者分享我们对于这些光辉的思想、精妙的见解和出色的洞察力的热情。’我做到了！…… ”

—— *Notices of the AMS, August 1999*

“拥有本书是一种快乐：大量的边栏注释、精美的照片、具有启迪性的图片、漂亮的素描画……阅读本书更是一种享受：清新惬意的风格、较低的阅读门槛、必备背景知识的适时提供、以及完美漂亮的证明。”

—— *LMS Newsletter, January 1999*

ISBN 978-7-04-026209-4

9 787040 262094 >

定价 34.00 元

学科类别：数学文化

网址：academic.hep.com.cn

Martin Aigner
Günter M. Ziegler 著

Proofs from THE BOOK

数学天书中的证明

(第三版)

附图 250 幅
含 Karl H. Hofmann 提供的插图

高等教育出版社
HIGHER EDUCATION PRESS

图字：01-2008-2746 号

图书在版编目 (CIP) 数据

数学天书中的证明: 第3版 / (德) 艾格纳 (Aigner, M.), (德) 齐格勒 (Ziegler, G.M.) 著; 冯荣权, 宋春伟, 宗传明译. —北京: 高等教育出版社, 2009.5
书名原文: Proofs from THE BOOK
ISBN 978-7-04-026209-4

Ⅰ. 数… Ⅱ. ①艾… ②齐… ③冯… ④宋… ⑤宗… Ⅲ. 数学–普及读物 Ⅳ. O1-49

中国版本图书馆 CIP 数据核字 (2009) 第 038637 号

策划编辑	王丽萍	责任编辑	李 鹏	封面设计	张 楠
版式设计	范晓红	责任校对	殷 然	责任印制	韩 刚

出版发行	高等教育出版社	购书热线	010-58581118
社 址	北京市西城区德外大街 4 号	免费咨询	400-810-0598
邮政编码	100120	网 址	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	中原出版传媒投资控股集团 北京汇林印务有限公司	畅想教育	http://www.widedu.com
开 本	850×1168 1/16	版 次	2009 年 5 月第 1 版
印 张	17.5	印 次	2009 年 5 月第 1 次印刷
字 数	320 000	定 价	34.00 元

物料号 26209-00

译者序

作为一门历史悠久的学问, 数学有她自身的文化和美学, 就像文学和艺术一样. 一方面, 数学家们在努力开拓新领域、解决老问题; 另一方面, 他们也在不断地从不同的角度反复学习、理解和欣赏前辈们的工作. 的确, 数学中有许多不仅值得反复推敲理解, 更值得细心品味和欣赏的杰作. 有些定理的证明不仅想法奇特、构思精巧, 作为一个整体更是天衣无缝. 难怪, 西方有些虔诚的数学家将这类杰作比喻为上帝的创造. 这也就是我们所说的数学天书中的证明.

本书介绍了 35 个著名数学问题的极富创造性和独具匠心的证明. 这不是一本教科书, 也不是一本专著, 而是一本开阔数学视野和提高数学修养的著作. 出于可读性的考虑, 本书侧重于研究生水平并且局限于数论、几何、分析、组合与图论五个数学领域. 但我确信, 每一个数学工作者都会喜欢这本书, 并且从中学到许多东西.

2002 年, 斯普林格出版社的高级编辑 Lindemann 博士来华访问时告诉我, 本书是斯普林格出版社近十年来最畅销的数学著作之一. 2005 年, 该出版社的 Heinze 博士来华访问时告诉我这本书已被翻译成 8 种文字出版, 同时他也希望我能促成这本著作中文版的出版. 高等教育出版社的王丽萍编辑对本书的出版给予了大力支持, 李鹏编辑细心核对了译稿并提出了许多改进意见. 冯荣权教授和宋春伟博士承担了翻译工作, 我负责统筹和校对. 陆珞和张姗姗对翻译工作给予了帮助.

宗传明

北京大学, 2008 年 9 月

中文版序言

本书的英文原著于 1998 年出版, 随即受到数学界的广泛好评, 并被陆续翻译成了十余种不同的文字, 其中包括法文、德文、意大利文、日文、西班牙文和俄文等.

中国曾经对世界文明作出过重要贡献. 中国的数学正处在一个迅速发展、人才辈出的时期. 我们很高兴本书中文版的问世, 并殷切希望她对中国数学的发展起到积极的作用. 中文版是在原著第三版的基础上翻译的. 我们诚挚地感谢宗传明教授、冯荣权教授和宋春伟博士为翻译这本书所做的各项努力.

Martin Aigner, Günter M. Ziegler

柏林, 2008 年 8 月

第一版序言

Paul Erdős 喜欢谈论数学天书 (《The Book》), 上帝在其中保存着数学定理的完美证明. 他这是根据 G. H. Hardy 的说法: 丑的数学是不会有永久地位的. Paul Erdős 也讲过, 作为数学家, 你可以不相信上帝, 但你应该相信数学天书. 几年前, 我们建议他勾画一下数学天书的轮廓. 他立即动手, 充满热情地一页一页提了很多建议. 本书原计划作为 Paul Erdős 的 85 岁生日献礼于 1998 年 3 月出版. 由于他于 1996 年夏天不幸去世, 他没有被列为我们的合作者. 而本书却是作为对他的纪念.



Paul Erdős



"*The Book*"

我们没有数学天书中的证明的定义或标准. 这里我们所呈现给大家的是一些具有高超的思想、聪明的观察和出色的洞察力的例子. 但愿读者与我们一样对它们富有热情并喜欢它们, 尽管我们的表述并不完美. 本书内容的选取, 在很大程度上受到 Paul Erdős 的影响. 其中许多章节是他建议的, 许多证明是他给出的或者源于他富有洞察力的问题或猜想. 所以, 这本书很大程度上反映了 Erdős 关于什么是数学天书中的证明的观点.

限制我们选题的一个因素是可读性: 本书中的所有章节应该能被具有大学数学水平的读者所理解. 一点线性代数、数学分析和数论以及一些离散数学的初等概念和思维方式就足够理解和欣赏本书的全部内容.

我们对那些为本书的出版提供过帮助和支持的人表示衷心的感谢 (其中包括初稿讨论班上的学生): Benno Artmann, Stephan Brandt, Stefan Felsner, Eli Goodman, Torsten Heldmann 和 Hans Mielke. 此外, Margrit Barrett, Christian Bressler, Ewgenij Gawrilow, Michael Joswig, Elke Pose, 和 Jörg Rambau 对本书的出版提供了技术支持, Tom Trotter 通读了初稿, Karl H. Hofmann 提供了一些优美的插图, 在此一并致谢. 当然, 我们要特别感谢已故的伟人 Paul Erdős 本人.

Martin Aigner, Günter M. Ziegler

柏林, 1998 年 3 月

第二版序言

本书的第一版受到了读者广泛的欢迎. 我们也收到了许多读者来信, 其中有的给出中肯的评论, 有的指出一些错误和缺陷, 有的则对另外的证明和新的讨论题目提出了很好的建议. (显然, 当我们希望展现完美证明时, 我们的表述并不完美).

本书的再版给我们提供了改善的机会: 新版增加了三章, 并对有的章节做了实质性的修改和给出新的证明, 同时还有一些小的改动. 这些改进不少是基于读者的建议. 另外, 我们删掉了第一版中关于“十三球问题”的一章, 因为该问题的完整证明需要很多细节, 很难做到简洁优美.

在此我们非常感谢那些来信的读者, 他们的来信对我们很有帮助, 他们中有 Stephan Brandt, Christian Elsholtz, Jürgen Elstrodt, Daniel Grieser, Roger Heath-Brown, Lee L. Keener, Christian Lebœuf, Hanfried Lenz, Nicolas Puech, John Scholes, Bernulf Weißbach 以及许多其他读者. 同样, 我们再次对Springer Heidelberg的 Ruth Allewelt 和 Karl-Friedrich Koch 以及柏林的 Christoph Eyrich 和 Torsten Heldmann 提供的帮助和支持表示衷心的感谢. Karl H. Hofmann 提供了一些高质量的新插图, 在此一并致谢.

Martin Aigner, Günter M. Ziegler

柏林, 2000 年 9 月

第三版序言

准备这本书的第一版时, 我们绝没想到出版后会有如此的成功. 自出版以来, 这本书已被翻译成许多种语言出版. 这期间我们收到了许多读者的热情来信, 其中有许多非常好的关于修改和增加新内容的建议 —— 这使我们忙了好几年.

第三版增加了两章 (分别关于 Euler 的分拆恒等式和洗牌), 关于 Euler 系列的三个证明成了独立的一章. 当然, 还有许多其他改进, 如 Calkinwilf-Newman 关于 "有理计数" 的处理. 目前也就是这些.

我们对过去五年中支持这一项目的每个人, 和对新版作出贡献的每个人表示衷心的感谢. 他们包括 David Bevan, Anders Björner, Dietrich Braess, John Cosgrave, Hubert Kalf, Günter Pickert, Alistair Sinclair 和 Herb Wilf.

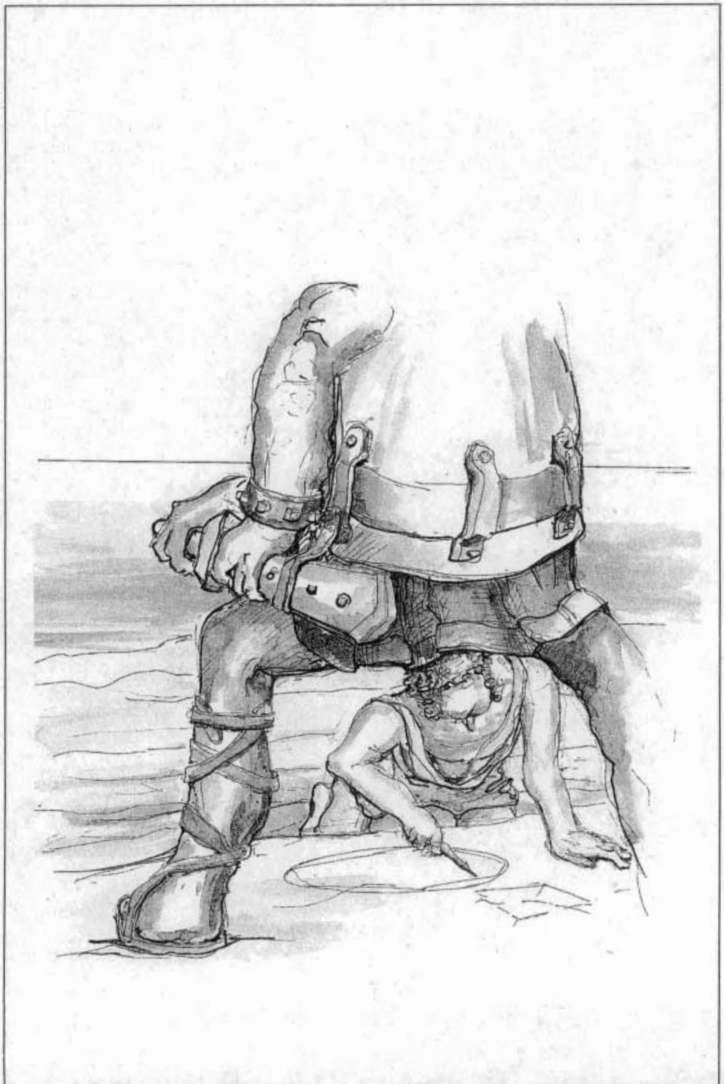
Martin Aigner, Günter M. Ziegler

柏林, 2003 年 7 月

目录

图论 221

数论



“无理性和 π”

素数无限的六种证明

第 1 章

让我们从最古老的天书证明开始. 通常人们将其归功于 Euclid (Elements IX, 20). 它告诉我们素数构成的数列永不终止.

■ Euclid 的证明. 对任何素数的有限集 $\{p_1, \cdots, p_r\}$, 考察 $n = p_1p_2\cdots p_r + 1$. 取 n 的素因子 p. 这个 p 不可能是任何一个 p_i: 否则 p 既是 n 的因子又是积 $p_1p_2\cdots p_r$ 的因子, 所以也是两者之差 $n - p_1p_2\cdots p_r = 1$ 的因子, 矛盾. 从而任何有限集 $\{p_1, \cdots, p_r\}$ 不可能包含所有的素数. □

在往下继续之前我们引入一些符号. 令 $\mathbb{N} = \{1, 2, 3, \cdots\}$ 为自然数集, $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ 为整数集, $\mathbb{P} = \{2, 3, 5, 7, \cdots\}$ 表示素数集.

下面我们介绍其他几种 (从一个长得多的单子上选出的) 不同的证明, 希望读者会像我们一样喜爱它们. 尽管它们来源于各异的观点, 其基本思想是相同的: 自然数没有上界, 而每个 $\geqslant 2$ 的自然数都有素因子. 这两个事实放在一起将导致 $\mathbb{P}$ 是无限的. 下一个证明归功于 Christian Goldbach (在 1730 年致 Leonhard Euler 的信里), 第三个证明显然是通俗的, 第四个是 Euler 自己给出的, 第五个由 Harry Fürstenberg 提出, 而最后一个是 Paul Erdős 的.

F_0	=	3
F_1	=	5
F_2	=	17
F_3	=	257
F_4	=	65537
F_5	=	$641 \cdot 6700417$

前几个 Fermat 数

■ 证明之二. 让我们先看看 *Fermat* 数 $F_n = 2^{2^n} + 1$, 这里 $n = 0, 1, 2, \cdots$. 下面证明任意两个 Fermat 数互素; 从而必有无穷多个素数. 为此我们只需验证递推关系

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \qquad (n \geqslant 1). \tag{1}$$

事实上, 设 m 是 F_k 和 F_n $(k < n)$ 的公因子, 则 m 整除 2, 于是 $m = 1$ 或者 2. 但由于 Fermat 数都是奇数, $m = 2$ 是不可能的.

现在我们用归纳法证明递归关系 (1): 当 $n = 1$ 时, 我们有 $F_0 = 3$ 及 $F_1 - 2 = 3$. 由归纳假设即得

Lagrange 定理

若 G 是一个有限 (乘法) 群且 U 是它的一个子群, 则必有 $|U|$ 整除 $|G|$.

■ **证明.** 考虑二元关系

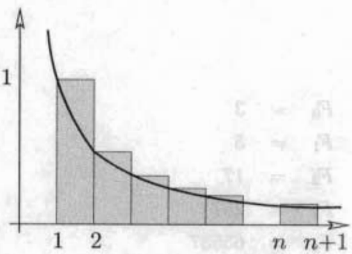
$$a \sim b : \Longleftrightarrow ba^{-1} \in U.$$

从群的定义易见 $\sim$ 是一个等价关系. 包含元素 a 的等价类即陪集

$$Ua = \{xa : x \in U\}.$$

显然 $|Ua| = |U|$, 所以 G 可以被划分为阶数均为 $|U|$ 的若干陪集, 从而可以导出 $|U|$ 整除 $|G|$. □

在 U 是循环子群 $\{a, a^2, \cdots, a^m\}$ 的特殊情况, 可见 m (使 $a^m = 1$ 的最小正整数, 称为元素 a 的阶) 一定整除 $|G|$ 的阶数.



在函数 $f(t) = \frac{1}{t}$ 上面的阶梯

$$\prod_{k=0}^{n} F_k = \Big(\prod_{k=0}^{n-1} F_k\Big) F_n = (F_n - 2)F_n$$
$$= (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

证毕. □

■ **证明之三.** 假设 $\mathbb{P}$ 有限且令 p 为最大的素数. 我们考虑*Mersenne* 数 $2^p - 1$, 并证明 $2^p - 1$ 的任意素因子 q 皆大于 p, 由此导出素数无限. 令 q 为整除 $2^p - 1$ 的一个素数, 则有 $2^p \equiv 1 \pmod{q}$. 因为 p 为素数, 前一公式说明在域 $\mathbb{Z}_q$ 的乘法群 $\mathbb{Z}_q \backslash \{0\}$ 中元素 2 的阶就是 p. 而该乘法群有 $q - 1$ 个元素. 由 Lagrange 定理, 我们得到 $p \,|\, (q-1)$ 并由此可以导出 $p < q$. □

下面是一个用到初等微积分的证明.

■ **证明之四.** 令 $\pi(x) := \#\{p \leqslant x : p \in \mathbb{P}\}$ 表示不超过实数 x 的素数个数. 将 $\mathbb{P} = \{p_1, p_2, p_3, \cdots\}$ 排为升序. 我们考虑由 $\log x = \int_1^x \frac{1}{t} dt$ 定义的自然对数 $\log x$.

现在将曲线 $f(t) = \frac{1}{t}$ 之下的面积与稍高的阶梯函数之下的面积进行比较. 对 $n \leqslant x < n+1$ 我们有

$$\log x \leqslant 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}$$
$$\leqslant \sum \frac{1}{m},$$

这里 $\sum$ 表示对所有的仅含 $p \leqslant x$ 的素因子的 $m \in \mathbb{N}$ 求和. 因为每个被求和的 m 可以唯一地表为 $\prod\limits_{p \leqslant x} p^{k_p}$ 的形式, 最后一个和式等于

$$\prod_{\substack{p \in \mathbb{P} \\ p \leqslant x}} \Big(\sum_{k \geqslant 0} \frac{1}{p^k}\Big).$$

由于上面的内和是公比为 $\frac{1}{p}$ 的几何级数, 所以

$$\log x \leqslant \prod_{\substack{p \in \mathbb{P} \\ p \leqslant x}} \frac{1}{1 - \frac{1}{p}} = \prod_{\substack{p \in \mathbb{P} \\ p \leqslant x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

显然, $p_k \geqslant k + 1$, 因而

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leqslant 1 + \frac{1}{k} = \frac{k+1}{k},$$

所以

$$\log x \leqslant \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x)+1.$$

众所周知 $\log x$ 无界, 所以 $\pi(x)$ 也无界, 从而素数有无穷多个. □

■ **证明之五.** 在用了分析之后现在轮到用拓扑了! 我们考虑整数集 $\mathbb{Z}$ 上的一种奇特的拓扑. 对 $a, b \in \mathbb{Z}, b>0$, 令

$$N_{a,b} = \{a+nb : n \in \mathbb{Z}\}.$$

每个集合 $N_{a,b}$ 都是正负无界的算术级数. 我们称集合 $O \subseteq \mathbb{Z}$ 为开集, 如果 O 是空集, 或者对任意的 $a \in O$ 存在 $b>0$ 使得 $N_{a,b} \subseteq O$. 显然, 开集的并总是开集. 另外, 如果 O_1 和 O_2 是两个开集, 对任意的 $a \in O_1 \cap O_2$, $N_{a,b_1} \subseteq O_1$ 以及 $N_{a,b_2} \subseteq O_2$, 都有 $a \in N_{a,b_1b_2} \subseteq O_1 \cap O_2$. 所以开集的有限交是开的. 从而我们定义的开集族的确导出了 $\mathbb{Z}$ 上的一个拓扑.

这里我们注意两个事实:

(A) 每个非空的开集都是无界的.

(B) 每个 $N_{a,b}$ 都是既开又闭的.

第一点是显然的. 至于第二点, 我们观察

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}.$$

这说明 $N_{a,b}$ 是开集的补, 因而是闭集.

素数在哪里呢? —— 下面就来了. 每个整数 $n \neq 1, -1$ 都有某个素因子 p, 所以我们有 $n \in N_{0,p}$ 以及

$$\mathbb{Z} \setminus \{1,-1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$



"掷扁石, 到无穷远"

如果 $\mathbb{P}$ 是有限的, 那么 $\bigcup_{p \in \mathbb{P}} N_{0,p}$ 将是有限个闭集的并 (根据 (B)), 所以是闭的. 进而可以导出 $\{1,-1\}$ 是一个开集, 这与 (A) 矛盾. □

■ **证明之六.** 我们的最后一个证明更迈进了一大步. 它不仅证明了素数无穷多, 还证明了无穷级数 $\sum_{p \in \mathbb{P}} \frac{1}{p}$ 发散. Euler 首次证明了这个重要的结果 (那个证明也很有趣), 我们将要介绍的是由 Erdős 给出的着实漂亮的证明.

令 $p_1, p_2, p_3, \cdots$ 表示升序排列的素数, 并假设 $\sum_{p \in \mathbb{P}} \frac{1}{p}$ 收敛. 那么一定存在自然数 k 使得 $\sum_{i \geqslant k+1} \frac{1}{p_i} < \frac{1}{2}$. 这时, 我们称 $p_1, \cdots, p_k$

为小素数, 称 $p_{k+1}, p_{k+2}, \cdots$ 为大素数. 这样对任意的自然数 N 都有

$$\sum_{i \geqslant k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{2}$$

令 N_b 表示满足 $n \leqslant N$ 且至少被一个大素数整除的正整数 n 的个数, N_s 表示满足 $n \leqslant N$ 且因子都是小素数的正整数的个数. 我们将证明存在某个 N 使得

$$N_b + N_s < N,$$

从而导出矛盾. 根据定义 $N_b + N_s$ 应该是等于 N 的.

为估计 N_b, 我们注意到 $\lfloor \frac{N}{p_i} \rfloor$ 计数了满足 $n \leqslant N$ 的 p_i 的倍数. 于是由 (2) 得到

$$N_b \leqslant \sum_{i \geqslant k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}. \tag{3}$$

现在再看 N_s. 把每个只有小素数因子的 $n \leqslant N$ 写成 $n = a_n b_n^2$ 的形式, 这里 a_n 是没有平方因子的部分. 每个 a_n 也就是一些互异的小素数的乘积, 所以一共恰好有 2^k 个可供选择的没有平方因子的部分. 另一方面, 由于 $b_n \leqslant \sqrt{n} \leqslant \sqrt{N}$, 至多有 $\sqrt{N}$ 个不同的平方部分, 所以

$$N_s \leqslant 2^k \sqrt{N}.$$

因为 (3) 对任意的 N 都成立, 只需找到一个满足 $2^k\sqrt{N} \leqslant \frac{N}{2}$ 亦即 $2^{k+1} \leqslant \sqrt{N}$ 的 N 就行了. 那么令 $N = 2^{2k+2}$ 即可. □

参考文献

[1] B. Artmann: *Euclid – The Creation of Mathematics,* Springer-Verlag, New York 1999.

[2] P. Erdős: *Über die Reihe* $\sum \frac{1}{p}$, Mathematica, Zutphen B **7** (1938), 1-2.

[3] L. Euler: *Introductio in Analysin Infinitorum,* Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8.

[4] H. Fürstenberg: *On the infinitude of primes,* Amer. Math. Monthly **62** (1955), 353.

Bertrand 假设

我们已经看到素数列 $2, 3, 5, 7, \cdots$ 是无限的. 其实, 素数列的间隙也无上限. 令 $N := 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p$ 表示所有小于 $k+2$ 的素数之积, 容易证明下面的 k 个数

$$N+2, N+3, N+4, \cdots, N+k, N+(k+1)$$

中没有素数. 因为满足 $2 \leqslant i \leqslant k+1$ 的 i 一定有小于 $k+2$ 的素因子. 该素因子必定整除 N, 所以也整除 $N+i$. 例如, 取 $k = 10$, 可以找到下面的 10 个相继整数

$$2312, 2313, 2314, \cdots, 2321,$$

其中没有素数.



Joseph Bertrand

但是素数序列的间隙还是有上界的. 一个著名的上界是这样描述的: "到下一个素数的距离不可能大于我们出发的这个数." 这就是 Bertrand 假设. Joseph Bertrand 提出了这个猜想并且验证了 $n < 3\,000\,000$ 的情形. 1850 年, Pafnuty Chebyshev 第一个对所有的 n 做出证明. 印度天才Ramanujan则给了一个简化得多的证明. 下面属于Paul Erdős 的天书证明取自 1932 年Erdős 发表的第一篇文章, 那时他 19 岁.



Beweis eines Satzes von Tschebyschef.

Von P. Erdős in Budapest.

Für den zuerst von Tschebyschef bewiesenen Satz, laut dessen es zwischen einer natürlichen Zahl und ihrer zweifachen stets wenigstens eine Primzahl gibt, liegen in der Literatur mehrere Beweise vor. Als einfachsten kann man ohne Zweifel den Beweis von Ramanujan[1]) bezeichnen. In seinem Werk *Vorlesungen über Zahlentheorie* (Leipzig, 1927), Band I, S. 66—68 gibt Herr Landau einen besonders einfachen Beweis für einen Satz über die Anzahl der Primzahlen unter einer gegebenen Grenze, aus welchem unmittelbar folgt, daß für ein geeignetes q zwischen einer natürlichen Zahl und ihrer q-fachen stets eine Primzahl liegt. Für die augenblicklichen Zwecken des Herrn Landau kommt es nicht auf die numerische Bestimmung der im Beweis auftretenden Konstanten an; man überzeugt sich aber durch eine numerische Verfolgung des Beweises leicht, daß q jedenfalls größer als 2 ausfällt.

In den folgenden Zeilen werde ich zeigen, daß man durch eine Verschärfung der dem Landauschen Beweis zugrunde liegenden Ideen zu einem Beweis des oben erwähnten Tschebyschefschen Satzes gelangen kann, der — wie mir scheint — an Einfachkeit nicht hinter dem Ramanujanschen Beweis steht. Griechische Buchstaben sollen im Folgenden durchwegs positive, lateinische Buchstaben natürliche Zahlen bezeichnen; die Bezeichnung p ist für Primzahlen vorbehalten.

1. Der Binomialkoeffizient

$$\binom{2a}{a} = \frac{(2a)!}{(a!)^2}$$

[1]) Sr. Ramanujan, A Proof of Bertrand's Postulate, *Journal of the Indian Mathematical Society*, 11 (1919), S. 181—182. — *Collected Papers of Srinivasa Ramanujan* (Cambridge, 1927), S. 208—209.

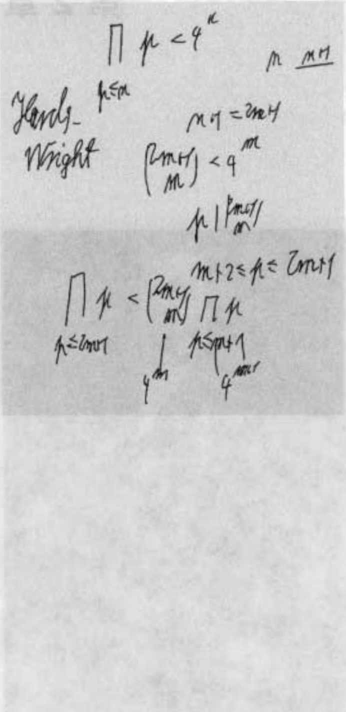
Bertrand 假设.

对每个 $n \geqslant 1$, 存在素数 p 满足 $n < p \leqslant 2n$.

■ **证明.** 我们足够仔细地估计 $\binom{2n}{n}$ 的大小, 将说明如果它没有满足 $n < p \leqslant 2n$ 的素因子, 它就会 "太小" 了. 以下分五步论证.

(1) 先对 $n < 4000$ 证明Bertrand假设. 这不必验证 4000 种情形: 只要 (这称作 "Landau技巧") 证实

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$



是一些素数且每一个均小于前一个的两倍. 这样每个区间 $\{y: n < y \leqslant 2n\}$, $n \leqslant 4000$, 就一定含有上面 14 个素数中的某个了.

(2) 下面证明

$$\prod_{p \leqslant x} p \ \leqslant\ 4^{x-1} \qquad \text{对所有实数} x \geqslant 2 \text{成立}. \tag{1}$$

这个证明对素数的个数进行归纳. 它并非来自 Erdős 的那篇文章, 但也是归功于 Erdős (见边栏), 是一个真正的天书证明.

首先注意到如果 q 是满足 $q \leqslant x$ 的最大素数, 那么

$$\prod_{p \leqslant x} p = \prod_{p \leqslant q} p \qquad \text{并且} \qquad 4^{q-1} \leqslant 4^{x-1}.$$

所以只需验证 (1) 当 $x = q$ 是素数时成立即可. 对 $q = 2$ 当然有 "$2 \leqslant 4$". 我们继续考虑 $q = 2m+1$(奇素数) 的情形. (这里我们可以归纳地假设 (1) 对所有 $\{2, 3, \cdots, 2m\}$ 中的整数 x 都成立.) 当 $q = 2m+1$ 时, 我们把乘积分成两部分可以得到

$$\begin{aligned}\prod_{p \leqslant 2m+1} p &= \prod_{p \leqslant m+1} p \cdot \prod_{m+1 < p \leqslant 2m+1} p \\ &\leqslant 4^m \binom{2m+1}{m} \\ &\leqslant 4^m 2^{2m} = 4^{2m}.\end{aligned}$$

事实上, 第一部分可由归纳假设得到

$$\prod_{p \leqslant m+1} p \leqslant 4^m.$$

而不等式

$$\prod_{m+1 < p \leqslant 2m+1} p \leqslant \binom{2m+1}{m}$$

成立则是因为 $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ 是个整数, 所考虑的素数都是分子 $(2m+1)!$ 的因子, 却不是分母 $m!(m+1)!$ 的因子. 最后,

$$\binom{2m+1}{m} \leqslant 2^{2m}$$

成立是因为

$$\binom{2m+1}{m} \text{ 与 } \binom{2m+1}{m+1}$$

是二项式展开

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}$$

中相等的两项.

(3) 根据Legendre定理 (见边栏), $\binom{2n}{n}=\frac{(2n)!}{n!n!}$ 中素因子 p 的次数恰好为

$$\sum_{k\geqslant 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor-2\left\lfloor\frac{n}{p^k}\right\rfloor\right).$$

和式中的每一项至多是 1, 因为

$$\left\lfloor\frac{2n}{p^k}\right\rfloor-2\left\lfloor\frac{n}{p^k}\right\rfloor \;<\; \frac{2n}{p^k}-2\left(\frac{n}{p^k}-1\right) \;=\; 2,$$

而且须是整数. 此外当 $p^k>2n$ 时就都为零了. 所以 $\binom{2n}{n}$ 中 p 的次数满足

$$\sum_{k\geqslant 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor-2\left\lfloor\frac{n}{p^k}\right\rfloor\right)\leqslant \max\{r: p^r\leqslant 2n\}.$$

所以整除 $\binom{2n}{n}$ 的 p 的次数不超过 $2n$. 特别地, 当 $p>\sqrt{2n}$ 时, 它在 $\binom{2n}{n}$ 中的次数最多为 1.

此外, Erdős 认为以下事实在他的证明中起到了关键作用: 满足 $\frac{2}{3}n<p\leqslant n$ 的素数 p 根本不会整除 $\binom{2n}{n}$! 事实上, $3p>2n$ 表明 (当 $n\geqslant 3$, 从而 $p\geqslant 3$) p 与 $2p$ 是仅有的两个出现在 $\frac{(2n)!}{n!n!}$ 的分子中的 p 的倍数, 这时在分母中也恰有 p 的 2 重因子.

(4) 现在可以估计 $\binom{2n}{n}$ 了. 当 $n\geqslant 3$ 时, 利用附录中对二项式系数的估计, 我们可以得到

$$\frac{4^n}{2n}\leqslant\binom{2n}{n}\leqslant\prod_{p\leqslant\sqrt{2n}}2n\cdot\prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n}p\cdot\prod_{n<p\leqslant 2n}p.$$

由于满足 $p\leqslant\sqrt{2n}$ 的素数不超过 $\sqrt{2n}$ 个, 从上式我们得到

$$4^n\leqslant(2n)^{1+\sqrt{2n}}\cdot\prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n}p\cdot\prod_{n<p\leqslant 2n}p. \qquad (2)$$

(5) 假设不存在素数 p 满足 $n<p\leqslant 2n$, 那么 (2) 中的最后一项乘积就是 1. 把 (1) 代入 (2) 我们得到

$$4^n\leqslant(2n)^{1+\sqrt{2n}}4^{\frac{2}{3}n}.$$

换言之,

$$4^{\frac{1}{3}n}\leqslant(2n)^{1+\sqrt{2n}}. \qquad (3)$$

Legendre 定理

$n!$ 中素数 p 的次数恰好为

$$\sum_{k\geqslant 1}\left\lfloor\frac{n}{p^k}\right\rfloor.$$

■ **证明.** 展开 $n!=1\cdot2\cdot3\cdot\cdots\cdot n$ 后的 n 项中恰有 $\lfloor\frac{n}{p}\rfloor$ 项被 p 整除, $\lfloor\frac{n}{p^2}\rfloor$ 项被 p^2 整除, 依此类推. 所以, $n!$ 中素数 p 的幂次为

$$\sum_{k\geqslant 1}\left\lfloor\frac{n}{p^k}\right\rfloor. \qquad \square$$

以下的例子

$\binom{26}{13}=2^3\cdot5^2\cdot7\cdot17\cdot19\cdot23$

$\binom{28}{14}=2^3\cdot3^3\cdot5^2\cdot17\cdot19\cdot23$

$\binom{30}{15}=2^4\cdot3^2\cdot5\cdot17\cdot19\cdot23\cdot29$

揭示了"非常小"的素数 $p<\sqrt{2n}$ 的高次幂可以整除 $\binom{2n}{n}$, 满足 $\sqrt{2n}<p\leqslant\frac{2}{3}n$ 的"小"素数最多是 $\binom{2n}{n}$ 的 1 重因子, 而在区间 $\frac{2}{3}n<p\leqslant n$ 内的素数则根本不会成为它的因子.

这对足够大的 n 是错误的! 事实上, 利用 $a+1<2^a$ (由归纳法这对所有的 $a\geqslant 2$ 成立) 我们有

$$2n=\left(\sqrt[6]{2n}\right)^6<\left(\lfloor\sqrt[6]{2n}\rfloor+1\right)^6<2^{6\lfloor\sqrt[6]{2n}\rfloor}\leqslant 2^{6\sqrt[6]{2n}}. \qquad (4)$$

所以对 $n\geqslant 50$ (从而 $18<2\sqrt{2n}$) 我们从 (3) 和 (4) 得到

$$2^{2n}\leqslant(2n)^{3\left(1+\sqrt{2n}\right)}<2^{\sqrt[6]{2n}\left(18+18\sqrt{2n}\right)}<2^{20\sqrt[6]{2n}\sqrt{2n}}=2^{20(2n)^{2/3}}.$$

这说明 $(2n)^{1/3}<20$, 从而要求 $n<4000$. □

从以上的估计中可以得到更多的事实. 基于 (2), 当 $n\geqslant 4000$ 时我们可以用同样的方法推导出

$$\prod_{n<p\leqslant 2n} p\geqslant 2^{\frac{1}{30}n}.$$

这样, 在 n 与 $2n$ 之间的素数个数至少是

$$\log_{2n}\left(2^{\frac{1}{30}n}\right)=\frac{1}{30}\frac{n}{\log_2 n+1}.$$

这个估计是蛮不错的. 在该区间内的素数个数大约是 $n/\log n$. 这可以从素数定理直接导出. 素数定理即:

$$\lim_{n\to\infty}\frac{\#\{p\leqslant n: p\text{是素数}\}}{n/\log n}=1.$$

这个著名结论是Hadamard 和de la Vallée-Poussin 最早在 1896 年证明的. Selberg和Erdős在 1948 年发现了一个初等证明 (没有使用复分析的工具, 但非常冗长复杂).

也许素数定理还不是最后的结果. 例如, Riemann 猜想 (见第 7 章的附录) 的解决将大大改进素数定理中的估计. 该猜想则是数学中最主要的有待解决的问题之一. 即使对 Bertrand 假设而言, 我们也可以期待明显的改进. 实际上, 下面也是一个著名的未解决问题:

在 n^2 与 $(n+1)^2$ 之间是否一定存在素数?

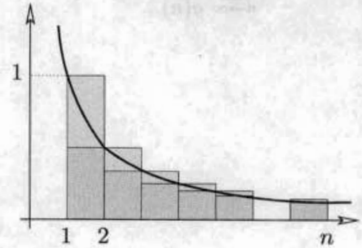
详见 [3, P19] 与 [4, PP. 248, 257].

附录: 一些估计

利用定积分估计

利用定积分估计和式是个简单而有效的方法 (在第 1 章证明之四我们已经看到过了). 为了估计调和级数

$$H_n = \sum_{k=1}^{n} \frac{1}{k},$$



我们在页边画出图形, 并通过比较曲线 $f(t) = \frac{1}{t}(1 \leqslant t \leqslant n)$ 之下的面积与深色矩形的面积得出

$$H_n - 1 = \sum_{k=2}^{n} \frac{1}{k} < \int_1^n \frac{1}{t}\,dt = \log n.$$

还可以通过比较曲线下的面积与高矩形 (浅色部分) 的面积得到

$$H_n - \frac{1}{n} = \sum_{k=1}^{n-1} \frac{1}{k} > \int_1^n \frac{1}{t}\,dt = \log n.$$

放在一起就有

$$\log n + \frac{1}{n} < H_n < \log n + 1.$$

这样, 我们就有 $\lim\limits_{n\to\infty} H_n \to \infty$ 并且 H_n 递增的阶由

$$\lim_{n\to\infty} \frac{H_n}{\log n} = 1$$

给出. 当然现在已知的估计 (参见 [2]) 要好得多, 例如

$$H_n = \log n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + O\left(\frac{1}{n^6}\right),$$

这里 $O\left(\frac{1}{n^6}\right)$ 表示对某个常数 c 满足 $f(n) \leqslant c\frac{1}{n^6}$ 的某个函数 $f(n)$.

其中 $\gamma \approx 0.5772$ 是 "Euler 常数".

阶乘的估计 —— Stirling 公式

同样的方法用于

$$\log(n!) = \log 2 + \log 3 + \cdots + \log n = \sum_{k=2}^{n} \log k$$

就得到

$$\log((n-1)!) < \int_1^n \log t\,dt < \log(n!).$$

$f(n) \sim g(n)$ 表示

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

这里定积分是易于计算的:

$$\int_1^n \log t\,dt \;=\; \Big[t\log t - t\Big]_1^n \;=\; n\log n - n + 1.$$

这样我们就得到 $n!$ 的一个下界

$$n! \;>\; e^{n\log n - n + 1} \;=\; e\Big(\frac{n}{e}\Big)^n.$$

同时也有上界

$$n! \;=\; n\,(n-1)! \;<\; ne^{n\log n - n+1} \;=\; en\Big(\frac{n}{e}\Big)^n.$$

想得到 *Stirling* 公式那样关于 $n!$ 的逼近

$$n! \;\sim\; \sqrt{2\pi n}\,\Big(\frac{n}{e}\Big)^n$$

则需要更仔细的分析. 更精确的估计也是有的, 例如

$$n! \;=\; \sqrt{2\pi n}\,\Big(\frac{n}{e}\Big)^n \left(1 + \frac{1}{12n} + \frac{1}{288n^2} - \frac{139}{5140n^3} + O\Big(\frac{1}{n^4}\Big)\right).$$

对二项式系数的估计

单从二项式系数 $\binom{n}{k}$ 的定义 (n- 集合的 k- 子集的个数) 出发, 我们就知道二项式系数的序列 $\binom{n}{0}, \binom{n}{1}, \cdots, \binom{n}{n}$ 满足

- 和式: $\sum\limits_{k=0}^{n} \binom{n}{k} = 2^n$
- 对称性: $\binom{n}{k} = \binom{n}{n-k}$.

从函数方程 $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$ 容易发现, 对固定的 n 而言, 二项式系数 $\binom{n}{k}$ 组成的序列是对称且单峰的: 向中部递增, 使得中间的二项式系数是序列中的最大项:

$$1 = \binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\lfloor n/2\rfloor} = \binom{n}{\lceil n/2\rceil} > \cdots > \binom{n}{n-1} > \binom{n}{n} = 1.$$

这里 $\lfloor x\rfloor$ 与 $\lceil x\rceil$ 分别代表实数 x 的下取整与上取整.

```
              1
            1   1
          1   2   1
        1   3   3   1
      1   4   6   4   1
    1   5  10  10   5   1
  1   6  15  20  15   6   1
1   7  21  35  35  21   7   1
```

Pascal 三角形

从上面提到的逼近公式我们可以得到对二项式系数相当精确的估计. 然而, 在本书中其实只需用到那些弱而简捷的估计. 例如: 对任意的 k, 有 $\binom{n}{k} \leqslant 2^n$; 对 $n \geqslant 2$, 有

$$\binom{n}{\lfloor n/2\rfloor} \geqslant \frac{2^n}{n},$$

等式成立仅当 $n = 2$. 特别地, 对 $n \geqslant 1$, 我们有

$$\binom{2n}{n} \geqslant \frac{4^n}{2n}.$$

上式成立是因为中间项 $\binom{n}{\lfloor n/2 \rfloor}$ 是序列 $\binom{n}{0}+\binom{n}{n}, \binom{n}{1}, \binom{n}{2}, \cdots, \binom{n}{n-1}$ 中最大的一个, 而序列的和是 2^n. 所以序列的均值是 $\frac{2^n}{n}$.

注意二项式系数的如下上界

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \leqslant \frac{n^k}{k!} \leqslant \frac{n^k}{2^{k-1}}.$$

这对序列首尾的那些 "小" 项是相当不错的估计, 尤其是当 n 比较大的时候 (相对于 k).

参考文献

[1] P. Erdős: *Beweis eines Satzes von Tschebyschef,* Acta Sci. Math. (Szeged) **5** (1930-32), 194-198.

[2] R. L. Graham, D. E. Knuth & O. Patashnik: *Concrete Mathematics. A Foundation for Computer Science*, Addison-Wesley, Reading MA 1989.

[3] G. H. Hardy & E. M. Wright: *An Introduction to the Theory of Numbers,* fifth edition, Oxford University Press 1979.

[4] P. Ribenboim: *The New Book of Prime Number Records,* Springer-Verlag, New York 1989.

等式成立仅当 $n = 2$. 特别地, 对 $n \geq 1$, 我们有

$$\frac{4^n}{2n} \leqslant \binom{2n}{n}$$

上式成立是因为中间项 $\binom{n}{\lfloor n/2\rfloor}$ 是序列 $\binom{n}{0}+\binom{n}{n}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ 中最大的一个, 而序列的和是 2^n, 所以序列的均值是 $\frac{2^n}{n}$.

注意二项式系数的如下上界

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \leqslant \frac{n^k}{k!} \leqslant \frac{n^k}{2^{k-1}}$$

这对序列首尾的那些"小"项是相当不错的估计, 尤其是当 n 比较大的时候 (相对于 k).

参考文献

[1] P. Erdős: *Beweis eines Satzes von Tschebyschef*, Acta Sci. Math. (Szeged) 5 (1930-32), 194-198.

[2] R. L. Graham, D. E. Knuth & O. Patashnik: *Concrete Mathematics. A Foundation for Computer Science*, Addison-Wesley, Reading MA 1989.

[3] G. H. Hardy & E. M. Wright: *An Introduction to the Theory of Numbers*, fifth edition, Oxford University Press 1979.

[4] P. Ribenboim: *The New Book of Prime Number Records*, Springer-Verlag, New York 1989.

二项式系数 (几乎) 非幂

第 3 章

这是 Bertrand 假设的一抹余韵, 引出了关于二项式系数的一个美妙结果. 1892 年, Sylvester 以下面的形式加强了 Bertrand 假设:

若 $n \geqslant 2k$, 则 $n, n-1, \cdots, n-k+1$ 中至少有一个具有比 k 大的素因子 p.

注意, 当 $n = 2k$ 时这恰好就是 Bertrand 假设. 1934 年, Erdős 基于他对 Bertrand 假设的证明, 用初等方法给出了 Sylvester 的结果的一个天书证明. Sylvester 定理 可以等价地叙述如下:

若 $n \geqslant 2k$, 则二项式系数

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

必有素因子 $p > k$.

有了这个观察, 我们来赏鉴 Erdős 的另一枚宝石. 什么时候会有 $\binom{n}{k}$ 等于某个幂 m^{ℓ}? 易见当 $k = \ell = 2$ 时, $\binom{n}{2} = m^2$ 有无穷多个解. 实际上, 若 $\binom{n}{2}$ 是平方数, 则 $\binom{(2n-1)^2}{2}$ 也是平方数: 令 $n(n-1) = 2m^2$, 则有

$$(2n-1)^2((2n-1)^2-1) = (2n-1)^2 4n(n-1) = 2(2m(2n-1))^2,$$

于是

$$\binom{(2n-1)^2}{2} = (2m(2n-1))^2.$$

从 $\binom{9}{2} = 6^2$ 开始我们可以得到无限多个解, 其中的下一个便是 $\binom{289}{2} = 204^2$. 当然, 这种方法并没有给出全部的解. 例如, 从 $\binom{50}{2} = 35^2$ 开始是另一个解的序列, $\binom{1682}{2} = 1189^2$ 又起始了另一列. 当 $k = 3$ 时, 已知的结果是 $\binom{n}{3} = m^2$ 有唯一解 $n = 50, m = 140$. 而我们到此为止了. 因为当 $k \geqslant 4$ 时, 对任意的 $\ell \geqslant 2$ 都不会有解, 这一结果是由 Erdős 巧妙地证明的.

$\binom{50}{3} = 140^2$ 是当 $k = 3, \ell = 2$ 时唯一的解

定理. *方程 $\binom{n}{k} = m^{\ell}$ 没有满足 $\ell \geqslant 2$ 及 $4 \leqslant k \leqslant n-4$ 的整数解.*

■ **证明.** 首先注意由 $\binom{n}{k}=\binom{n}{n-k}$, 我们不妨假设 $n\geqslant 2k$. 假设定理不成立, 令 $\binom{n}{k}=m^\ell$, 我们的证明分四步导出矛盾.

(1) 由 Sylvester 定理, $\binom{n}{k}$ 有大于 k 的素因子 p, 所以 p^ℓ 整除 $n(n-1)\cdots(n-k+1)$. 显然, 仅有一个 $n-i$ 是 p 的倍数 (由 $p>k$), 所以有 $p^\ell\,|\,(n-i)$, 进而

$$n\ \geqslant\ p^\ell\ >\ k^\ell\ \geqslant\ k^2.$$

(2) 任取分子的一项 $n-j$ 并将其写成形如 $n-j=a_jm_j^\ell$, 其中 a_j 不被任何非平凡的 ℓ- 幂整除. 由**(1)**可知, a_j 仅有不超过 k 的素因子. 下面我们证明对 $i\neq j$ 总有 $a_i\neq a_j$. 假设不然, 存在 $i<j$ 满足 $a_i=a_j$, 则有 $m_i\geqslant m_j+1$ 以及

$$\begin{aligned} k\ &>\ (n-i)-(n-j)\ =\ a_j(m_i^\ell-m_j^\ell)\ \geqslant\ a_j((m_j+1)^\ell-m_j^\ell)\\ &>\ a_j\ell m_j^{\ell-1}\ \geqslant\ \ell(a_jm_j^\ell)^{1/2}\ \geqslant\ \ell(n-k+1)^{1/2}\\ &\geqslant\ \ell(\tfrac{n}{2}+1)^{1/2}\ >\ n^{1/2}, \end{aligned}$$

与 **(1)** 中的 $n>k^2$ 相矛盾.

(3) 下面我们证明这些 a_i 是 $1,2,\cdots,k$ 的一个重排 (根据 Erdős, 这是整个证明的关键). 既然已知它们各自不同, 只需证明

$$a_0a_1\cdots a_{k-1}\,|\,k!.$$

将 $n-j=a_jm_j^\ell$ 代入方程 $\binom{n}{k}=m^\ell$, 得到

$$a_0a_1\cdots a_{k-1}(m_0m_1\cdots m_{k-1})^\ell\ =\ k!m^\ell.$$

两边将 $m_0\cdots m_{k-1}$ 和 m 的公因子约去, 我们得到

$$a_0a_1\cdots a_{k-1}u^\ell\ =\ k!v^\ell,$$

其中 $\gcd(u,v)=1$. 下面只需证明 $v=1$. 假设不然, 令 p 为 v 的某个素因子. 由于 $\gcd(u,v)=1$, 素数 p 一定是 $a_0a_1\cdots a_{k-1}$ 的素因子, 所以由 **(1)** 它一定小于或等于 k. 由 Legendre 定理 (见第 2 章), $k!$ 包含 p 作为因子的重数是 $\sum_{i\geqslant 1}\lfloor\frac{k}{p^i}\rfloor$. 现在我们估计一下 p 在 $n(n-1)\cdots(n-k+1)$ 里作为因子的重数. 设 i 为正整数, $b_1<b_2<\cdots<b_s$ 是 $n,n-1,\cdots,n-k+1$ 里面 p^i 的倍数. 这时 $b_s=b_1+(s-1)p^i$, 我们得到

$$(s-1)p^i\ =\ b_s-b_1\ \leqslant\ n-(n-k+1)\ =\ k-1,$$

进而

$$s \leqslant \left\lfloor \frac{k-1}{p^i} \right\rfloor + 1 \leqslant \left\lfloor \frac{k}{p^i} \right\rfloor + 1.$$

所以 $n, \cdots, n-k+1$ 中 p^i 的倍数的个数以及 $a_0, a_1, \cdots, a_{k-1}$ 中 p^i 的倍数的个数有上界 $\lfloor \frac{k}{p^i} \rfloor + 1$. 用在第 2 章中的 Legendre 定理所用的论证可以得出 $a_0 a_1 \cdots a_{k-1}$ 中因子 p 的次数至多是

$$\sum_{i=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right).$$

唯一的差别是这里求和停止在 $i = \ell - 1$, 这是因为 a_j 不含有 ℓ 次幂.

综合以上的考虑, p 在 v^ℓ 中的重数至多是

$$\sum_{i=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right) - \sum_{i \geqslant 1} \left\lfloor \frac{k}{p^i} \right\rfloor \leqslant \ell - 1.$$

这就导出了我们想要的矛盾.

现在已经可以解决 $\ell = 2$ 的情形了. 事实上, 由 $k \geqslant 4$, 某个 a_i 就等于 4. 这与各个 a_i 都不含平方因子相矛盾. 所以下面我们就假设 $\ell \geqslant 3$.

到此为止的分析适用于 $\binom{50}{3} = 140^2$, 由于

$50 = 2 \cdot 5^2$
$49 = 1 \cdot 7^2$
$48 = 3 \cdot 4^2$

且 $5 \cdot 7 \cdot 4 = 140$.

(4) 由于 $k \geqslant 4$, 一定存在 3 个指标 i_1, i_2, i_3 满足 $a_{i_1} = 1, a_{i_2} = 2, a_{i_3} = 4$. 换言之,

$$n - i_1 = m_1^\ell, \; n - i_2 = 2m_2^\ell, \; n - i_3 = 4m_3^\ell.$$

我们断言: $(n-i_2)^2 \neq (n-i_1)(n-i_3)$. 设若不然, 我们记 $b = n - i_2$, $n - i_1 = b - x$ 和 $n - i_3 = b + y$, 其中 $0 < |x|, |y| < k$. 那么

$$b^2 = (b-x)(b+y) \quad \text{或} \quad (y-x)b = xy,$$

显然 $x = y$ 是不可能成立的. 然后由第 **(1)** 步就有

$$|xy| = b|y-x| \geqslant b > n-k > (k-1)^2 \geqslant |xy|.$$

这是不可能的.

现在有 $m_2^2 \neq m_1 m_3$. 不妨设 $m_2^2 > m_1 m_3$ (否则证明类似), 继续最后的推导. 我们得到

$$\begin{aligned}
2(k-1)n &> n^2 - (n-k+1)^2 \\
&> (n-i_2)^2 - (n-i_1)(n-i_3) \\
&= 4[m_2^{2\ell} - (m_1 m_3)^\ell] \\
&\geqslant 4[(m_1 m_3 + 1)^\ell - (m_1 m_3)^\ell] \\
&\geqslant 4\ell m_1^{\ell-1} m_3^{\ell-1}.
\end{aligned}$$

由 $\ell \geqslant 3$ 且 $n > k^{\ell} \geqslant k^3 > 6k$, 我们可以进一步得到

$$\begin{aligned} 2(k-1)nm_1m_3 &> 4\ell m_1^{\ell}m_3^{\ell} = \ell(n-i_1)(n-i_3) \\ &> \ell(n-k+1)^2 > 3(n-\frac{n}{6})^2 \\ &> 2n^2. \end{aligned}$$

此时因为 $m_i \leqslant n^{1/\ell} \leqslant n^{1/3}$ 我们就最终得到了

$$kn^{2/3} \geqslant km_1m_3 > (k-1)m_1m_3 > n,$$

从而 $k^3 > n$. 这与 **(1)** 的结论相矛盾. 这个矛盾说明最初的假设不成立, 证毕. □

参考文献

[1] P. Erdős: *A theorem of Sylvester and Schur,* J. London Math. Soc. **9** (1934), 282-288.

[2] P. Erdős: *On a diophantine equation,* J. London Math. Soc. **26** (1951), 176-178.

[3] J. J. Sylvester: *On arithmetical series,* Messenger of Math. **21** (1892), 1-19, 87-120; Collected Mathematical Papers Vol. 4, 1912, 687-731.

表自然数为平方和

第 4 章

哪些自然数可以写为两个平方数之和?

$1 = 1^2 + 0^2$
$2 = 1^2 + 1^2$
$3 =$??
$4 = 2^2 + 0^2$
$5 = 2^2 + 1^2$
$6 =$??
$7 =$??
$8 = 2^2 + 2^2$
$9 = 3^2 +$
$10 = 3^2 +$
$11 =$??
⋮

此问题与数论本身一样古老, 它的解决是本领域中的经典. "困难" 的部分在于解决形如 $4m+1$ 的素数可表为平方和. G. H. Hardy 写道, Fermat 的*平方和定理* "非常公正地说, 可列为数论中最好的结果之一." 虽然如此, 下面的天书证明是相当新的.

让我们先 "预热" 一下. 首先, 我们将要把素数 $p=2$, 形如 $p=4m+1$ 的素数, 以及形如 $p=4m+3$ 的素数区分开. 每个素数恰属于这三类之一. 此时注意到 (用 "欧几里得式" 的方法) 存在无穷多个形如 $4m+3$ 的素数. 实际上, 假如仅有有限多个, 则可以取这种形式的最大素数 p_k. 置

$$N_k \ := \ 2^2 \cdot 3 \cdot 5 \cdots p_k - 1$$

(其中 $p_1 = 2, p_2 = 3, p_3 = 5, \cdots$ 表示所有不同素数), 则有 N_k 同余于 $3 \,(\mathrm{mod}\, 4)$, 所以其必有素因子 $4m+3$, 而这个素因子比 p_k 大, 矛盾. 本章之末我们还将证明, 形如 $p=4m+1$ 的素数也有无穷多个.

第一条引理是著名的 "互反律" 的一个特例: 它刻画了那些使 -1 在 $\mathbb{Z}_p$ 中是某个元素的平方的那些素数 p (引理证明的后面框内有相关的回顾).



Pierre de Fermat

引理 1. *方程* $s^2 \equiv -1 \,(\mathrm{mod}\, p)$ *对素数* $p = 4m+1$ *有两个解* $s \in \{1, 2, \cdots, p-1\}$; *对* $p=2$ *有一个解; 对形如* $p = 4m+3$ *的素数无解.*

■ **证明.** 当 $p=2$ 时取 $s=1$. 对奇素数 p, 我们定义 $\{1, 2, \cdots, p-1\}$ 上的如下等价关系: 每个元素的等价类由它在 $\mathbb{Z}_p$ 中的加法逆和乘法逆生成. 这样 "一般的" 等价类包含四个元素

$$\{x, -x, \overline{x}, -\overline{x}\}.$$

以上的 4 元集包含它的每个元素的两种逆. 然而, 还有更小的等价类. 我们注意到如果所列四个元素并非互异, 这种情况就会发生.

- 对奇的 p, $x \equiv -x$ 不可能发生.
- $x \equiv \overline{x}$ 等价于 $x^2 \equiv 1$. 这有两个解: $x=1$ 与 $x=p-1$, 对应等价类是 $\{1, p-1\}$.
- $x \equiv -\overline{x}$ 等价于 $x^2 \equiv -1$. 这个方程或者无解, 或者仅有两个解 $x_0, p-x_0$: 这种情况下的等价类是$\{x_0, p-x_0\}$.

当 $p=11$ 时对应的分类为 $\{1,10\}, \{2,9,6,5\}, \{3,8,4,7\}$; 当 $p=13$ 时分类为 $\{1,12\}, \{2,11,7,6\}, \{3,10,9,4\}, \{5,8\}$: 数对 $\{5,8\}$ 给出了 $s^2 \equiv -1 \bmod 13$ 的两个解.

集合 $\{1,2,\cdots,p-1\}$ 有 $p-1$ 个元素. 将它分成四元组 (大小为 4 的等价类) 和 1 或 2 个二元组 (大小为 2 的等价类). 当 $p-1=4m+2$, 仅能有一个二元组 $\{1, p-1\}$, 其他的均为四元组, 因而 $s^2 \equiv -1 \pmod p$ 无解. 当 $p-1=4m$ 时则必有另一个二元组, 这就是 $s^2 \equiv -1$ 的两个解. □

现在, 让我们 "忙中偷闲" 看一下如下结论: 对所有素数 p, 方程

$$x^2+y^2 \equiv -1 \pmod p$$

总有解. 事实上, $\mathbb{Z}_p$ 中有 $\lfloor \frac{p}{2} \rfloor + 1$ 个形如 x^2 的互异元素, $\lfloor \frac{p}{2} \rfloor + 1$ 个形如 $-(1+y^2)$ 的互异元素. 因为 $\mathbb{Z}_p$ 仅有 p 个元素, 所以一定存在 x 和 y 满足

$$x^2 \equiv -(1+y^2) \pmod p.$$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_5$ 中的加法和乘法

素域

当 p 为一个素数, 集合 $\mathbb{Z}_p = \{0, 1, \cdots, p-1\}$ 上 "模 p" 的加法和乘法构成一个有限域. 我们将需要以下简单性质:

- 对 $x \in \mathbb{Z}_p, x \neq 0$, 加法逆 (表为 $-x$) 由 $p-x \in \{1,2,\cdots,p-1\}$ 给出. 若 $p>2$, 那么 x 和 $-x$ 是 $\mathbb{Z}_p$ 中互异的元素.
- 每个 $x \in \mathbb{Z}_p \backslash \{0\}$ 有唯一的乘法逆 $\overline{x} \in \mathbb{Z}_p \backslash \{0\}$, 使得 $x\overline{x} \equiv 1 \pmod p$.
  素数的特性保证了 $\mathbb{Z}_p \to \mathbb{Z}_p, z \mapsto xz$ 对 $x \neq 0$ 是单射. 所以在有限集合 $\mathbb{Z}_p \backslash \{0\}$ 这个映射也是满的, 从而每个 x 有唯一的逆 $\overline{x} \neq 0$ 使得 $x\overline{x} \equiv 1 \pmod p$.
- 对 $h = \lfloor \frac{p}{2} \rfloor$, $\mathbb{Z}_p$ 中的平方数 $0^2, 1^2, 2^2, \cdots, h^2$ 两两互异.
  这是因为 $x^2 \equiv y^2$ 将导致 $x \equiv y$ 或 $x \equiv -y$. 这 $1 + \lfloor \frac{p}{2} \rfloor$ 个元素 $0^2, 1^2, \cdots, h^2$ 称为 $\mathbb{Z}_p$ 中的平方.

引理 2. *形如 $n = 4m+3$ 的自然数不能表为两个平方之和.*

■ **证明.** 偶数的平方总有 $(2k)^2 = 4k^2 \equiv 0 \pmod 4$, 奇数的平方则有 $(2k+1)^2 = 4(k^2+k)+1 \equiv 1 \pmod 4$. 因此, 两个平方数之和模 4 只能同余于 0, 1 或 2. □

这已足以表明形如 $p = 4m+3$ 的素数是"差的". 那么, 我们继续来讨论形如 $p = 4m+1$ 的素数的"好"性质. 在导出主要定理的过程中, 下面是关键的一步.

命题. *每个形如 $p = 4m+1$ 的素数都是两个平方数之和. 亦即存在 $x, y \in \mathbb{N}$ 使得 $p = x^2 + y^2$ 成立.*

我们介绍这一结果的两个证明, 它们同样地优美动人. 第一个证明巧妙地利用了"鸽笼原理" (在引理 2 之前我们已经"忙中偷闲"地用过一次了. 关于鸽笼原理详见第 22 章), 此外还聪明地运用了"模 p"而又再回来的论证. 这个思想归功于挪威数论学家 Axel Thue.

■ **证明.** 考虑满足 $0 \leqslant x', y' \leqslant \sqrt{p}$ 的整数对 (x', y'), 换言之, $x', y' \in \{0, 1, \cdots, \lfloor\sqrt{p}\rfloor\}$. 共有 $(\lfloor\sqrt{p}\rfloor + 1)^2$ 个这样的对. 由于 $\lfloor x \rfloor + 1 > x$, 令 $x = \sqrt{p}$, 可知这样的整数对比 p 多. 所以对任意 $s \in \mathbb{Z}$, 由所有的对 (x', y') 计算出的值 $x' - sy'$ 在模 p 的意义下不可能两两互异. 换言之, 对每个 s 必有两个不同的对

$$(x', y'),\ (x'', y'') \ \in \ \{0, 1, \cdots, \lfloor\sqrt{p}\rfloor\}^2$$

满足

$$x' - sy' \ \equiv \ x'' - sy'' \pmod p.$$

当 $p = 13$, 有 $\lfloor\sqrt{p}\rfloor = 3$, 我们考察 $x', y' \in \{0, 1, 2, 3\}$. 对 $s = 5$, $x' - sy' \pmod{13}$ 顺次取下表中的值:

x' \ y'	0	1	2	3
0	0	8	3	11
1	1	9	4	12
2	2	10	5	0
3	3	11	6	1

取其差, 我们得到 $x' - x'' \equiv s(y' - y'') \pmod p$. 定义

$$x := |x' - x''|, \quad y := |y' - y''|,$$

我们可以得到

$$(x, y) \in \{0, 1, \cdots, \lfloor\sqrt{p}\rfloor\}^2 \quad 且 \quad x \equiv \pm sy \pmod p.$$

又因为 (x', y') 和 (x'', y'') 是不同的整数对, 所以 x 与 y 不可能都为 0.

在引理 1 的保证下我们取 s 为 $s^2 \equiv -1 \pmod p$ 的一个解, 则有 $x^2 \equiv s^2y^2 \equiv -y^2 \pmod p$, 从而得到

$$(x, y) \in \mathbb{Z}^2 \quad 满足 \quad 0 < x^2 + y^2 < 2p \quad 和 \quad x^2 + y^2 \equiv 0 \pmod p.$$

由于 p 是 0 与 $2p$ 之间唯一被 p 整除的数. 所以 $x^2+y^2=p$. 证毕! □

我们的第二个证明显然也是天书证明, 是 1971 年由 Roger Heath-Brown 发现的, 到 1984 年才为世人所知. (Don Zagier 又给出了一个浓缩版的"一行证明".) 这也是一个初等证明, 我们甚至不需要用到引理 1.

Heath-Brown 的论证依赖三个线性对合: 第一个相当显然, 第二个不易发现, 第三个是平凡的但给出"最后一击". 想象不到的是, 第二个对合对应着方程 $4xy+z^2=p$ 的整数解集的某种暗藏结构.

■ **证明.** 研究集合

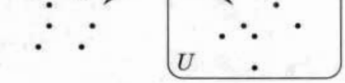
$$S \;:=\; \{(x,y,z)\in\mathbb{Z}^3 : 4xy+z^2=p,\quad x>0,\quad y>0\}.$$

这是个有限集. 事实上, $x\geqslant 1$ 与 $y\geqslant 1$ 表明 $y\leqslant \frac{p}{4}$ 及 $x\leqslant\frac{p}{4}$. 所以 x 和 y 都只有有限多个可能的取值, 而一旦给定 x 和 y, z 至多有两种取值.

1. 第一个线性对合定义如下

$$f: S\longrightarrow S,\quad (x,y,z)\longmapsto(y,x,-z).$$

也就是说, "互换 x 和 y, 再把 z 变成负的". 这显然是从 S 到自身的映射, 还是对合: 应用两次, 结果是单位映射. 并且 f 没有不动点, 这是因为 $z=0$ 将使得 $p=4xy$ 导致矛盾. 此外, f 把



$$T \;:=\; \{(x,y,z)\in S : z>0\}$$

中的解恰好映到 $S\backslash T$ 中的解, 即满足 $z<0$ 的解. 最后, f 同时改变了 $x-y$ 和 z 的符号, 所以它把

$$U \;:=\; \{(x,y,z)\in S : (x-y)+z>0\}$$

中的解恰好映到 $S\backslash U$ 中的解. 关于这一点我们需要确认没有满足 $(x-y)+z=0$ 的解, 好在假如有解的话将有 $p=4xy+z^2=4xy+(x-y)^2=(x+y)^2$.

我们从研究 f 的过程中得到了什么? 主要的观察是既然 f 把 T 和 U 分别映到它们的补, 它也使 $T\backslash U$ 和 $U\backslash T$ 中的元素相互交换. 换言之, 在 U 中但不在 T 中的元素与在 T 中却不在 U 中的元素一样多, 所以 T 和 U 基数相同.

2. 第二个是集合 U 上的一个对合:

$$g: U \longrightarrow U, \quad (x,y,z) \longmapsto (x-y+z, y, 2y-z).$$

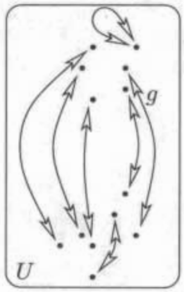
首先检验这个映射定义的合理性: 若 $(x,y,z) \in U$, 则有 $x-y+z>0, y>0$ 且 $4(x-y+z)y+(2y-z)^2 = 4xy+z^2$, 故 $g(x,y,z) \in S$. 由 $(x-y+z)-y+(2y-z) = x > 0$ 也确实有 $g(x,y,z) \in U$.

另外, g 是一个对合: $g(x,y,z) = (x-y+z, y, 2y-z)$ 被 g 映到 $((x-y+z)-y+(2y-z), y, 2y-(2y-z)) = (x,y,z)$.

最后, g 恰有 1 个不动点: 显然

$$(x,y,z) \;=\; g(x,y,z) \;=\; (x-y+z, y, 2y-z)$$

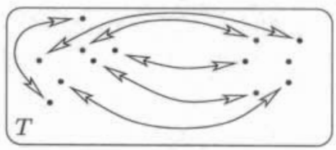
在 $y=z$ 时成立. 但此时 $p = 4xy+y^2 = (4x+y)y$ 要求 $y=1=z$ 及 $x = \frac{p-1}{4}$.



容易看出, 当 g 是 U 上的一个对合且恰有 1 个不动点, 则 U 的基数必为奇数.

3. 第三个, 集合 T 上互换 x 与 y 的对合:

$$h: T \longrightarrow T, \quad (x,y,z) \longmapsto (y,x,z).$$



在基数为奇的有限集上, 每个对合至少有一个不动点.

这个映射显然是合理定义的, 且是一个对合. 我们把关于前两个对合的信息综合起来: T 的基数等于 U, 是个奇数. 然而, 如果 h 是奇基数有限集上的一个对合, 那它一定有不动点. 综上所述, 存在一个点 $(x,y,z) \in T$ 满足 $x=y$. 它就是

$$p = 4x^2 + z^2 = (2x)^2 + z^2$$

的解. □

注意, 这个证明还告诉我们, 形如 $p = 4m+1$ 的素数 p 可以表为 $p = x^2 + (2y)^2$ 的个数是奇的. (这种表示其实是唯一的, 见 [3].) 另外这两个证明都不是有效的: 当 p 是一个十多位的素数时就很难找出 x 和 y 了! 关于有效地表素数为两个平方和的方法参见 [1] 和 [7].

下面的定理完全回答了本章开始时所提出的问题.

定理. 自然数 n 可表示为两个平方和的形式当且仅当 n 的每个形如 $p = 4m+3$ 的素因子的重数都是偶数.

■ **证明.** 为方便起见, 我们称 n 为可表的, 如果存在 $x, y \in \mathbb{N}_0$ 使得 $n = x^2 + y^2$. 这个定理是以下五个结果的推论.

(1) $1 = 1^2 + 0^2$ 及 $2 = 1^2 + 1^2$ 是可表的. 每个形如 $p = 4m+1$ 的素数是可表的.

(2) 两个可表的数 $n_1 = x_1^2 + y_1^2$ 与 $n_2 = x_2^2 + y_2^2$ 的乘积是可表的: $n_1 n_2 = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2$.

(3) 若 n 是可表的, $n = x^2 + y^2$, 则 nz^2 也可表: $nz^2 = (xz)^2 + (yz)^2$.

结果 (1), (2) 与 (3) 放在一起就证明了充分性部分.

(4) 若素数 $p = 4m + 3$ 整除可表的整数 $n = x^2 + y^2$, 则 p 既整除 x 也整除 y, 从而 p^2 整除 n. 事实上, 若有 $x \not\equiv 0 \,(\mathrm{mod}\, p)$, 则可以找到 $\overline{x}$ 满足 $x\overline{x} \equiv 1 \,(\mathrm{mod}\, p)$. 在方程 $x^2 + y^2 \equiv 0$ 两端同乘以 $\overline{x}^2$, 我们得到

$$1 + y^2\overline{x}^2 = 1 + (\overline{x}y)^2 \equiv 0 \,(\mathrm{mod}\, p),$$

由引理 1, 对 $p = 4m + 3$ 这不可能.

(5) 若 n 可表, 且 $p = 4m + 3$ 整除 n, 则 p^2 整除 n, 从而 n/p^2 也可表. 这由 (4) 即得. 定理证毕. □

作为推论, 我们得到有无穷多个形如 $p = 4m + 1$ 的素数. 为此考虑同余于 $1 \,(\mathrm{mod}\, 4)$ 的数

$$M_k = (3 \cdot 5 \cdot 7 \cdots p_k)^2 + 2^2.$$

它所有的素因子都大于 p_k, 又由前面证明中的事实 (4) 可知它没有形如 $4m + 3$ 的素因子. 所以 M_k 有形如 $4m + 1$ 的素因子, 且比 p_k 大.

我们以两则评论结束本章:

- 若 a 和 b 是互素的两个自然数, 则存在无穷多个形如 $am+b$ ($m \in \mathbb{N}$) 的素数 —— 这是Dirichlet的一个著名 (且困难的) 定理. 更准确地说, 可以证明当 x 足够大时, 形如 $p = am + b$ 且满足 $p \leqslant x$ 的素数的个数可相当精确地由函数 $\frac{1}{\varphi(a)} \frac{x}{\log x}$ 所描述, 这里 $\varphi(a)$ 表示满足 $1 \leqslant b < a$ 且与 a 互素的 b 的个数. (这是对我们在第 2 章中提到过的素数定理的一个显著改进.)
- 这说明当 a 固定, 由不同的 b 产生的素数出现的几率本质上是相等的. 然而, 比如当 $a = 4$ 时可以观察到一个相当微小但仍然是显著的持续的趋势 —— “更多” 素数形如 $4m + 3$, 也即随机取一个大的 x, 那么更可能是满足 $p \leqslant x$ 且形如 $p = 4m + 3$ 的素数比形如 $p = 4m + 1$ 的素数多. 这个现象被称作 “Chebyshev 偏差”; 见 Riesel [4] 及 Rubinstein 与 Sarnak [5].

参考文献

[1] F. W. Clarke, W. N. Everitt, L. L. Littlejohn & S. J. R. Vorster: *H. J. S. Smith and the Fermat Two Squares Theorem,* Amer. Math. Monthly **106** (1999), 652-665.

[2] D. R. Heath-Brown: *Fermat's two squares theorem,* Invariant (1984), 2-5.

[3] I. Niven & H. S. Zuckerman: *An Introduction to the Theory of Numbers,* Fifth edition, Wiley, New York 1972.

[4] H. Riesel: *Prime Numbers and Computer Methods for Factorization,* Second edition, Progress in Mathematics **126**, Birkhäuser, Boston MA 1994.

[5] M. Rubinstein & P. Sarnak: *Chebyshev's bias,* Experimental Mathematics **3** (1994), 173-197.

[6] A. Thue: *Et par antydninger til en taltheoretisk metode,* Kra. Vidensk. Selsk. Forh. **7** (1902), 57-75.

[7] S. Wagon: *Editor's corner: The Euclidean algorithm strikes again,* Amer. Math. Monthly **97** (1990), 125-129.

[8] D. Zagier: *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares,* Amer. Math. Monthly **97** (1990), 144.

有限除环即为域

第 5 章



Ernst Witt

环是近世代数中的重要结构. 若环 R 有乘法单位元 1, 且每个非零元有乘法逆, 称 R 为*除环*. 所以, R 比域缺少的就是乘法的交换性. 关于非交换除环最好的例子是 Hamilton 发现的四元数环. 但如本章题目所揭示的, 那样的除环必定是无限的. 如果 R 有限, 诸公理将迫使乘法为可交换的.

这个如今已成为经典的结果曾经令众多数学家神往, 正如 Herstein 写下的: "它把某个代数系统里的元素数目与那系统的乘法这两个看似毫不相干的事物联系起来, 真是太出人意料了."

定理. *每个有限除环 R 都是可交换的.*

这个通常归功于 MacLagan Wedderburn 的美丽定理已经被许多人用各种各样的思想证明过了. Wedderburn 本人即在 1905 年给出了三个证明, 同年, Leonard E. Dickson 也发现了一个证明. 后来, Emil Artin, Hans Zassenhaus, Nicolas Bourbaki 以及其他很多人也给出了证明. 有一个证明由于简洁优美脱颖而出. 这是 1931 年由 Ernst Witt 发现的. 该证明把两个初等思想综合在一起取得辉煌成功.

■ **证明.** 我们的第一件配料是把线性代数和基础群论拌在一起. 对任意的元素 $s \in R$, 令 C_s 表示与 s 可交换的元素的集合 $\{x \in R : xs = sx\}$; C_s 称为 s 的*中心化子*. 显然, C_s 包含 0 和 1, 是 R 的子除环. *中心* Z 则是 R 中与所有元素交换的元素的集合, 也就是 $Z = \bigcap_{s \in R} C_s$. 特别地, Z 是可交换的且 0 与 1 在 Z 中, 故 Z 是个*有限域*. 我们假定 $|Z| = q$.

将 R 和 C_s 分别看作域 Z 上的向量空间. 令 n 为向量空间 R 的维数, 可以导出 $|R| = q^n$. 类似地, 对某个合适的整数 $n_s \geqslant 1$, 我们有 $|C_s| = q^{n_s}$.

现在假设 R 不是域. 这意味着存在某个 $s \in R$, 其中心化子 C_s 不是全部的 R, 或者说 $n_s < n$.

在集合 $R^* := R\backslash\{0\}$ 上考虑关系

$$r' \sim r \quad :\Longleftrightarrow \quad r' = x^{-1}rx \ \text{对某个}\ x \in R^*.$$

易见 $\sim$ 是一个等价关系. 令

$$A_s := \{x^{-1}sx : x \in R^*\}$$

表示含有 s 的等价类. 我们注意到 $|A_s| = 1$ 当且仅当 s 在中心 Z 中. 所以根据我们的假设, 存在满足 $|A_s| \geqslant 2$ 的 A_s. 固定 $s \in R^*$, 考察从 R^* 到 A_s 的满射 $f_s : x \longmapsto x^{-1}sx$. 对 $x, y \in R^*$ 我们发现

$$\begin{aligned} x^{-1}sx = y^{-1}sy &\iff (yx^{-1})s = s(yx^{-1}) \\ &\iff yx^{-1} \in C_s^* \iff y \in C_s^* x. \end{aligned}$$

上式中 $C_s^* := C_s\backslash\{0\}$, 且 $C_s^* x = \{zx : z \in C_s^*\}$ 的大小是 $|C_s^*|$. 故每个 $x^{-1}sx$ 在映射 f_s 下恰好是 R^* 中 $|C_s^*| = q^{n_s} - 1$ 个元素的像, 从而 $|R^*| = |A_s|\,|C_s^*|$. 特别地, 注意

$$\frac{|R^*|}{|C_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |A_s| \quad \text{对所有的}\ s\ \text{都是整数}.$$

我们知道等价类是对 R^* 的分拆. 把 Z^* 里的元素合在一起, 用 $A_1, \cdots, A_t$ 代表那些含有多于 1 个元素的等价类. 由我们的假设可知 $t \geqslant 1$. 因为 $|R^*| = |Z^*| + \sum_{k=1}^{t} |A_k|$, 我们就证明了所谓的类数公式

$$q^n - 1 = q - 1 + \sum_{k=1}^{t} \frac{q^n - 1}{q^{n_k} - 1}, \tag{1}$$

其中对所有的 k 都有 $1 < \frac{q^n-1}{q^{n_k}-1} \in \mathbb{N}$.

从 (1) 我们就离开抽象代数回到自然数中. 下面断言 $(q^{n_k} - 1) \mid (q^n - 1)$ 表明 $n_k \mid n$. 事实上, 记 $n = an_k + r$, 其中 $0 \leqslant r < n_k$, 则 $(q^{n_k} - 1) \mid (q^{an_k + r} - 1)$ 说明

$$(q^{n_k} - 1) \mid ((q^{an_k+r} - 1) - (q^{n_k} - 1)) = q^{n_k}(q^{(a-1)n_k + r} - 1).$$

从而由 q^{n_k} 与 $q^{n_k} - 1$ 互素, 我们可以导出 $(q^{n_k} - 1) \mid (q^{(a-1)n_k+r} - 1)$. 继续下去直到 $(q^{n_k} - 1) \mid (q^r - 1)$. 然而当 $0 \leqslant r < n_k$ 时唯一可能的情形就是 $r = 0$, 亦即 $n_k \mid n$. 总结一下, 我们得到

$$n_k \mid n \quad \text{对每个}\ k. \tag{2}$$

单位根

任意复数 $z = x + iy$ 可以写成极坐标形式

$$z = re^{i\varphi} = r(\cos\varphi + i\sin\varphi),$$

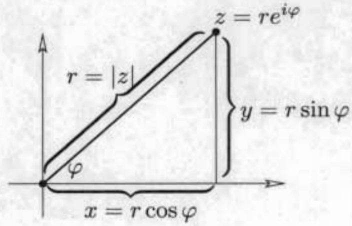
其中 $r = |z| = \sqrt{x^2 + y^2}$ 是 z 到原点的距离, φ 是从 x- 正半轴量出的夹角. 所以 n- 次单位根就形如

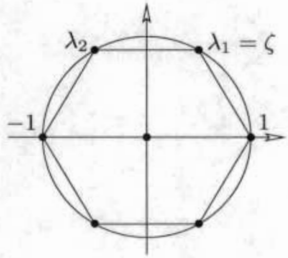
$$\lambda_k = e^{\frac{2k\pi i}{n}} = \cos(2k\pi/n) + i\sin(2k\pi/n), \qquad 0 \leqslant k \leqslant n-1.$$

对所有的 k 都有

$$\lambda_k^n = e^{2k\pi i} = \cos(2k\pi) + i\sin(2k\pi) = 1.$$

通过把一个正 n- 边形内嵌入单位圆我们就得到这些根. 注意到对每个 k, $\lambda_k = \zeta^k$, 这里 $\zeta = e^{\frac{2\pi i}{n}}$. 从而 n- 次单位根组成一个阶为 n 的循环群 $\{\zeta, \zeta^2, \cdots, \zeta^{n-1}, \zeta^n = 1\}$.





当 $n = 6$ 时的单位根

现在第二件配料来了: 复数域 $\mathbb{C}$. 考察多项式 $x^n - 1$, 它在 $\mathbb{C}$ 中的根称为 n-次单位根. 由 $\lambda^n = 1$, 所有的根 λ 满足 $|\lambda| = 1$. 所以, 它们都在复平面的单位圆周上. 事实上, 它们正是复数 $\lambda_k = e^{\frac{2k\pi i}{n}} = \cos(2k\pi/n) + i\sin(2k\pi/n), 0 \leqslant k \leqslant n-1$ (参见框格). 有的根 λ 对某个 $d < n$ 满足 $\lambda^d = 1$; 例如 $\lambda = -1$ 满足 $\lambda^2 = 1$. 对根 λ, 令 d 为使得 $\lambda^d = 1$ 成立的最小正整数. 换言之, d 即 λ 在单位根群中的阶. 那么由 Lagrange 定理, $d \mid n$ (“每个元素的阶整除群的阶”, 见第 1 章中的边栏). 注意到阶为 n 的根总是存在的, 比方说 $\lambda_1 = e^{\frac{2\pi i}{n}}$.

现在我们把 d 次单位根放在一起, 且定义

$$\phi_d(x) := \prod_{\lambda \text{ 是 } d \text{ 次的}} (x - \lambda).$$

这样 $\phi_d(x)$ 的定义与 n 无关. 因为每个根都有某个阶 d, 可见

$$x^n - 1 = \prod_{d \mid n} \phi_d(x). \tag{3}$$

关键的观察是: 多项式 $\phi_n(x)$ 的系数都是整数(或者说对任意的 n, 有 $\phi_n(x) \in \mathbb{Z}[x]$), 此外它的常数项是 1 或 -1.

让我们仔细验证一下以上的断言. 当 $n=1$ 时只有 1 这一个根, 因此 $\phi_1(x)=x-1$. 用归纳法: 假设对所有的 $d<n$ 已经有 $\phi_d(x)\in\mathbb{Z}[x]$ 并且 $\phi_d(x)$ 的常数项是 1 或 -1. 由 (3) 我们得到

$$x^n-1 \;=\; p(x)\,\phi_n(x) \tag{4}$$

其中 $p(x)=\sum\limits_{j=0}^{\ell}p_jx^j$, $\phi_n(x)=\sum\limits_{k=0}^{n-\ell}a_kx^k$, 且 $p_0=1$ 或 $p_0=-1$.

由 $-1=p_0a_0$, 我们容易得出 $a_0\in\{1,-1\}$. 假设已有 $a_0,a_1,\cdots,a_{k-1}\in\mathbb{Z}$. 通过计算 (4) 的两端 x^k 项的系数, 我们得到

$$\sum_{j=0}^{k}p_ja_{k-j} \;=\; \sum_{j=1}^{k}p_ja_{k-j}+p_0a_k \;\in\mathbb{Z}.$$

由归纳假设, 所有的 $a_0,\cdots,a_{k-1}$ (以及所有的 p_j) 在 $\mathbb{Z}$ 里面. 所以再由 p_0 是 1 或 -1 就得到了 a_k 必为整数.

我们已为最后一击做好准备了. 取 (1) 式中的某个数 $n_k\,|\,n$, 则

$$x^n-1 \;=\; \prod_{d\,|\,n}\phi_d(x) \;=\; (x^{n_k}-1)\phi_n(x)\prod_{d\,|\,n,\,d\nmid n_k,\,d\neq n}\phi_d(x).$$

从而在 $\mathbb{Z}$ 中有整除关系

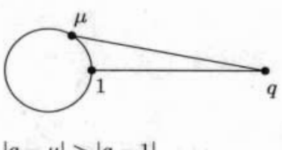
$$\phi_n(q)\,|\,(q^n-1) \qquad 及 \qquad \phi_n(q)\,\Big|\,\frac{q^n-1}{q^{n_k}-1}. \tag{5}$$

因为 (5) 对所有的 k 都成立, 从类数公式 (1) 我们得到

$$\phi_n(q)\,|\,(q-1).$$

这不可能成立. 为什么呢? 我们知道 $\phi_n(x)=\prod(x-\lambda)$, 其中 λ 取遍 x^n-1 的所有 n 次根. 令 $\widetilde{\lambda}=a+ib$ 为这样的一个根. 由 $n>1$ (假设 $R\neq Z$) 我们有 $\widetilde{\lambda}\neq1$, 这表明实部 a 比 1 小. 再由 $|\widetilde{\lambda}|^2=a^2+b^2=1$ 我们得到

$$\begin{aligned}|q-\widetilde{\lambda}|^2 &= |q-a-ib|^2 \;=\; (q-a)^2+b^2\\ &= q^2-2aq+a^2+b^2 \;=\; q^2-2aq+1\\ &> q^2-2q+1 \qquad (由\, a<1)\\ &= (q-1)^2.\end{aligned}$$



$|q-\mu|>|q-1|$

所以 $|q-\widetilde{\lambda}|>q-1$ 对所有 n 次根成立. 从而

$$|\phi_n(q)| = \prod_{\lambda} |q - \lambda| > q - 1,$$

意味着 $\phi_n(q)$ 不可能是 $q-1$ 的因子, 矛盾, 证毕. □

参考文献

[1] L. E. Dickson: *On finite algebras,* Nachrichten der Akad. Wissenschaften Göttingen Math.-Phys. Klasse (1905), 1-36; Collected Mathematical Papers Vol. III, Chelsea Publ. Comp, The Bronx, NY 1975, 539-574.

[2] J. H. M. Wedderburn: *A theorem on finite algebras,* Trans. Amer. Math. Soc. **6** (1905), 349-352.

[3] E. Witt: *Über die Kommutativität endlicher Schiefkörper,* Abh. Math. Sem. Univ. Hamburg **8** (1931), 413.

一些无理数

第 6 章

"π 是无理数"

当亚里士多德断言圆的直径和周长不可公度的时候就已提出了这个猜想. 这个基本结论的第一个证明是由Johann Heinrich Lambert于 1766 年给出的. 我们的证明属于Ivan Niven (1947 年): 一个只需用到初等微积分且极其优美的一页纸证明. 它富有思想, 正如 Iwamoto 和 Koksma 分别指出的那样, 还可从中得到更多的东西. 例如

- π^2 是无理数;
- 对任意的有理数 $r \neq 0$, e^r 是无理数.

当然, Niven 的方法的确另有根源和先驱: 它可以追溯到 1873 年 Charles Hermite 的经典文章, 在那里首先证实了 e 是超越数, 亦即 e 不是任何有理系数多项式的根.



Charles Hermite

$$e := 1+\frac{1}{1}+\frac{1}{2}+\frac{1}{6}+\frac{1}{24}+\cdots$$
$$= 2.718281828...$$

在处理 π 之前我们先看看 e 和它的幂, 证明它们是无理数. 这还要早得多, 让我们根据这些结果发展的历史顺序来介绍.

作为开头, 很容易看出 (像 Fourier 在 1815 年那样) $e = \sum_{k\geqslant 0} \frac{1}{k!}$ 是无理数. 事实上, 若存在整数 a 与 $b > 0$ 使得 $e = \frac{a}{b}$, 则有

$$n!be = n!a$$

对每个 $n \geqslant 0$ 都成立. 但这是不可能的, 因为一方面在等号的右方的确是一个整数, 另一方面依据

$$e = \Big(1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}\Big)+\Big(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\frac{1}{(n+3)!}+\cdots\Big)$$

等号左方可分解为一个整数部分

$$bn!\Big(1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}\Big)$$

和另一部分

$$b\Big(\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}+\cdots\Big).$$

几何级数

对无穷的几何级数

$$Q = \frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^3} + \cdots,$$

当 $q > 1$ 时显然有

$$qQ = 1 + \frac{1}{q} + \frac{1}{q^2} + \cdots = 1 + Q,$$

于是

$$Q = \frac{1}{q-1}.$$



192 JOURNAL DE MATHÉMATIQUES

SUR L'IRRATIONNALITÉ DU NOMBRE

$e = 2,718\ldots;$

PAR J. LIOUVILLE.

On prouve dans les éléments que le nombre e, base des logarithmes népériens, n'a pas une valeur rationnelle. On devrait, ce me semble, ajouter que la même méthode prouve aussi que e ne peut pas être racine d'une équation du second degré à coefficients rationnels, en sorte que l'on ne peut pas avoir $ae + \frac{b}{e} = c$, a étant un entier positif et b, c, des entiers positifs ou négatifs. En effet, si l'on remplace dans cette équation e et $\frac{1}{e}$ ou e^{-1} par leurs développements déduits de celui de e^x, puis qu'on multiplie les deux membres par $1.2.3\ldots n$, on trouvera aisément

$$\frac{a}{n+1}\left(1 + \frac{1}{n+2} + \ldots\right) \pm \frac{b}{n+1}\left(1 - \frac{1}{n+2} + \ldots\right) = \mu,$$

μ étant un entier. On peut toujours faire en sorte que le facteur

$$\pm\frac{b}{n+1}$$

soit positif; il suffira de supposer n pair si b est <0 et n impair si b est >0; en prenant de plus n très grand, l'équation que nous venons d'écrire conduira dès lors à une absurdité; car son premier membre étant essentiellement positif et très petit, sera compris entre 0 et 1, et ne pourra pas être égal à un entier μ. Donc, etc.

Liouville 的文章

第二部分大约是 $\frac{b}{n}$, 所以当 n 很大时就不会是整数. 其实它比 $\frac{b}{n+1}$ 大, 比 $\frac{b}{n}$ 小, 这可以通过与一个几何级数作比较看出来:

$$\begin{aligned}\frac{1}{n+1} &< \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \cdots \\ &< \frac{1}{n+1} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + \cdots = \frac{1}{n}.\end{aligned}$$

现在也许有人会想这个简单乘 $n!$ 的技巧恐怕对证 e^2 是无理数也不足. 这是个更强的命题: $\sqrt{2}$ 就是一个例子, 其本身是无理数, 平方之后却不是.

然而, 从 John Cosgrave 那里我们学到, 利用两个漂亮的思想/观察 (不妨称为 "技巧") 还是可以迈进两步: 每个技巧都足以证明 e^2 是无理数, 综合在一起还可以解决 e^4. 第一个技巧是在 J. Liouville 于 1840 年发表的一篇仅有一页纸的文章里发现的 —— 第二个则包含在一个两页的 "附录" 里, 那是 Liouville 发表在接下去的两张纸上的.

为什么 e^2 是无理数? 我们可以从 $e^2 = \frac{a}{b}$ 中推导出什么? 根据 Liouville 我们应该这样写

$$be = ae^{-1},$$

作替换

$$e = 1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120} + \cdots$$

及

$$e^{-1} = 1 - \frac{1}{1} + \frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120} \pm \cdots,$$

然后对足够大的偶数 n 在两边同乘 $n!$. 接着就看到 $n!be$ 几乎是个整数:

$$n!b\left(1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n!}\right)$$

是整数, 而剩下的部分

$$n!b\left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots\right)$$

大约是 $\frac{b}{n}$: 它比 $\frac{b}{n+1}$ 大, 比 $\frac{b}{n}$ 小, 后一点是我们刚刚计算过的.

与此同时 $n!ae^{-1}$ 也几乎是个整数: 我们也是有一个大的整数部分, 以及大约是 $(-1)^{n+1}\frac{a}{n}$ 的另一部分

$$(-1)^{n+1}n!a\left(\frac{1}{(n+1)!} - \frac{1}{(n+2)!} + \frac{1}{(n+3)!} \mp \cdots\right).$$

更准确地说: 对偶数 n, 另一部分比 $-\frac{a}{n}$ 为大, 但比

$$-a\Big(\frac{1}{n+1}-\frac{1}{(n+1)^2}-\frac{1}{(n+1)^3}-\cdots\Big)=-\frac{a}{n+1}\Big(1-\frac{1}{n}\Big)<0$$

小. 但是这不可能成立: 因为当 n 是很大的偶数时, 这表明 $n!ae^{-1}$ 比一个整数小那么一点点, 而 $n!be$ 比一个整数大一点点. 因此 $n!ae^{-1}=n!be$ 是不可能的. □

为证明 e^4 是无理数, 我们大胆假设 $e^4=\frac{a}{b}$ 是有理数, 再写为

$$be^2 \;=\; ae^{-2}.$$

现在可以对比较大的 n 在两端同乘 $n!$, 然后再收集非整数的部分和. 但是这回不再有效: 左端剩余项的和大约是 $b\frac{2^{n+1}}{n}$, 而右端则是 $(-1)^{n+1}a\frac{2^{n+1}}{n}$, 两者都随着 n 的增大变得很大.

所以对这种情形我们必须更加仔细, 并在策略上加两个调整: 首先不再取任意的比较大的 n, 而是取 2 的一个大的幂次 $n=2^m$; 其次不再同乘 $n!$, 而是代之以 $\frac{n!}{2^{n-1}}$. 另外需要一个小小的引理, 即 Legendre 定理的一个特殊情形 (见第 2 章): 对任意的 $n\geqslant 1$, 整数 $n!$ 中素因子 2 的次数最多是 $n-1$ —— 当 (且仅当)n 是 2 的幂, 即形如 $n=2^m$ 时等式成立.

引理不难验证: $n!$ 的 $\lfloor\frac{n}{2}\rfloor$ 个因子是偶数, $\lfloor\frac{n}{4}\rfloor$ 个因子可被 4 整除, 以此类推. 因此若 2^k 是满足 $2^k\leqslant n$ 的最大的 2 的幂, 则 $n!$ 中素因子 2 的次数为

$$\Big\lfloor\frac{n}{2}\Big\rfloor+\Big\lfloor\frac{n}{4}\Big\rfloor+\cdots+\Big\lfloor\frac{n}{2^k}\Big\rfloor\;\leqslant\;\frac{n}{2}+\frac{n}{4}+\cdots+\frac{n}{2^k}\;=\;n\Big(1-\frac{1}{2^k}\Big)\;\leqslant\;n-1$$

且两个等号刚好当 $n=2^k$ 时成立.

回到 $be^2=ae^{-2}$. 我们观察

$$b\frac{n!}{2^{n-1}}e^2 \;=\; a\frac{n!}{2^{n-1}}e^{-2} \tag{1}$$

并代入级数

$$e^2 \;=\; 1+\frac{2}{1}+\frac{4}{2}+\frac{8}{6}+\cdots+\frac{2^r}{r!}+\cdots$$

及

$$e^{-2} \;=\; 1-\frac{2}{1}+\frac{4}{2}-\frac{8}{6}\pm\cdots+(-1)^r\frac{2^r}{r!}+\cdots.$$

当 $r\leqslant n$ 时, 我们分别取两边的整数项并做和即得到

$$b\frac{n!}{2^{n-1}}\frac{2^r}{r!} \quad 与 \quad (-1)^r a\frac{n!}{2^{n-1}}\frac{2^r}{r!}.$$

当 $r>0$ 时分母 $r!$ 含素因子 2 至多 $r-1$ 重, 而 $n!$ 则含恰好 $n-1$ 重. (故当 $r>0$ 时这些项都是偶数.)

又由于 n 是偶数 (取定 $n=2^m$), (1) 中两个级数的 $r\geqslant n+1$ 部分分别是

$$2b\Big(\frac{2}{n+1}+\frac{4}{(n+1)(n+2)}+\frac{8}{(n+1)(n+2)(n+3)}+\dots\Big)$$

与

$$2a\Big(-\frac{2}{n+1}+\frac{4}{(n+1)(n+2)}-\frac{8}{(n+1)(n+2)(n+3)}\pm\cdots\Big).$$

再次通过与几何级数做比较, 这两个级数当 n 足够大时分别近似于 $\frac{4b}{n}$ 与 $-\frac{4a}{n}$. 对很大的 $n=2^m$, 这表明 (1) 的左端比一个整数大一点, 而右端比一个整数小一点 —— 矛盾! □

所以我们得到 e^4 是无理数. 欲证 e^3, e^5 等等也是无理数, 则需要更多的工具 (也就是一点微积分) 以及一个新的想法 —— 这本质上可追溯到Charles Hermite, 其关键之处藏在下面这个简单的引理之中.

引理. 对某个取定的 $n\geqslant 1$, 令

$$f(x) \;=\; \frac{x^n(1-x)^n}{n!}.$$

(i) 函数 $f(x)$ 是个多项式, 且形如 $f(x)=\frac{1}{n!}\sum_{i=n}^{2n}c_ix^i$, 其系数 c_i 都是整数.

(ii) 当 $0<x<1$ 时, 有 $0<f(x)<\frac{1}{n!}$.

(iii) 对所有的 $k\geqslant 0$, 微分取值 $f^{(k)}(0)$ 和 $f^{(k)}(1)$ 都是整数.

■ **证明.** 第 (i), (ii) 部分是显然的.

对 (iii), 注意到由 (i), 除非 $n\leqslant k\leqslant 2n$, k 次导数 $f^{(k)}$ 在 $x=0$ 处的取值必为零. 而当 $n\leqslant k\leqslant 2n$ 时, $f^{(k)}(0)=\frac{k!}{n!}c_k$ 确为整数. 由于 $f(x)=f(1-x)$, 对任意的 x, 我们有 $f^{(k)}(x)=(-1)^kf^{(k)}(1-x)$. 所以 $f^{(k)}(1)=(-1)^kf^{(k)}(0)$ 也都是整数.

定理 1. 对任意的 $r\in\mathbb{Q}\backslash\{0\}$, e^r 是无理数.

■ **证明.** 我们只须证明对正整数 s, e^s 不可能是有理数 (若 $e^{\frac{s}{t}}$ 是有理数, 则 $\big(e^{\frac{s}{t}}\big)^t=e^s$ 也将是有理数). 假设存在整数 $a,b>0$, 使得 $e^s=\frac{a}{b}$, 取 n 足够大满足 $n!>as^{2n+1}$. 我们定义

估计 $n!>e(\frac{n}{e})^n$ 使我们得到一个 "足够大" 的显式 n.

$$F(x) \;:=\; s^{2n}f(x)-s^{2n-1}f'(x)+s^{2n-2}f''(x)\mp\cdots+f^{(2n)}(x),$$

其中 $f(x)$ 是引理中的函数. 既然当 $k > 2n$ 时的高阶导数 $f^{(k)}(x)$ 都是零, $F(x)$ 也可写为无限和的形式

$$F(x) \;=\; s^{2n}f(x) - s^{2n-1}f'(x) + s^{2n-2}f''(x) \mp \cdots .$$

从而我们看到多项式 $F(x)$ 满足恒等式

$$F'(x) \;=\; -s\,F(x) + s^{2n+1}f(x).$$

所以, 我们有

$$\frac{d}{dx}\left[e^{sx}F(x)\right] \;=\; se^{sx}F(x) + e^{sx}F'(x) \;=\; s^{2n+1}e^{sx}f(x)$$

以及

$$N \;:=\; b\int_0^1 s^{2n+1}e^{sx}f(x)dx \;=\; b\left[e^{sx}F(x)\right]_0^1 \;=\; aF(1) - bF(0).$$

由引理的 (iii), $F(0)$ 和 $F(1)$ 都是整数, 故 N 是整数. 不过, 引理的 (ii) 也给 N 的上下界提供了估计:

$$0 < N = b\int_0^1 s^{2n+1}e^{sx}f(x)dx \;<\; bs^{2n+1}e^s\frac{1}{n!} \;=\; \frac{as^{2n+1}}{n!} \;<\; 1.$$

这样 N 不可能是整数: 矛盾. □

既然这个技巧如此成功, 我们再用一次.

定理 2. *π^2 是无理数.*

■ **证明.** 假设对整数 $a, b > 0$ 有 $\pi^2 = \frac{a}{b}$. 此处我们利用多项式

$$F(x) \;:=\; b^n\Big(\pi^{2n}f(x) - \pi^{2n-2}f^{(2)}(x) + \pi^{2n-4}f^{(4)}(x) \mp \cdots\Big),$$

容易验证它满足 $F''(x) = -\pi^2F(x) + b^n\pi^{2n+2}f(x)$.

从引理的 (iii) 已经知道 $F(0)$ 和 $F(1)$ 都是整数. 基本的微分法则告诉我们

$$\begin{aligned}\frac{d}{dx}\big[F'(x)\sin\pi x - \pi F(x)\cos\pi x\big] &= \big(F''(x) + \pi^2F(x)\big)\sin\pi x\\ &= b^n\pi^{2n+2}f(x)\sin\pi x\\ &= \pi^2a^nf(x)\sin\pi x,\end{aligned}$$

于是得到

$$\begin{aligned}N := \pi\int_0^1 a^nf(x)\sin\pi x\,dx &= \left[\frac{1}{\pi}F'(x)\sin\pi x - F(x)\cos\pi x\right]_0^1\\ &= F(0) + F(1),\end{aligned}$$

π 不是有理数, 但它确实可以用有理数进行 “好的近似”, 其中一些从古时起即为人们所知:

$$\begin{aligned}\tfrac{22}{7} &= 3.142857142857\ldots\\ \tfrac{355}{113} &= 3.141592920353\ldots\\ \tfrac{104348}{33215} &= 3.141592653921\ldots\\ \pi &= 3.141592653589\ldots\end{aligned}$$

是个整数. 此外, N 是正的, 因为它是一个正函数 (除掉边界) 的一个定积分. 然而, 若取 n 足够大使得 $\frac{\pi a^n}{n!}<1$, 则由引理的 (ii) 推得

$$0 \; < \; N \; = \; \pi \int_0^1 a^n f(x) \sin \pi x \, dx \; < \; \frac{\pi a^n}{n!} \; < \; 1,$$

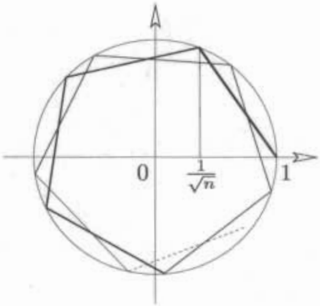
矛盾. □

以下是我们最后一个有关无理数的结果.

定理 3. *对每个奇整数 $n \geqslant 3$, 如下定义的数*

$$A(n) \; := \; \frac{1}{\pi} \arccos\left(\frac{1}{\sqrt{n}}\right)$$

是无理数.



我们将在Hilbert的第三问题 (见第 8 章) 里面需要这个结果的两种情形 $n=3$ 和 $n=9$. 对 $n=2$ 和 $n=4$ 我们有 $A(2)=\frac{1}{4}$ 及 $A(4)=\frac{1}{3}$, 所以限制在奇整数上是要紧的. 这些数值易从边上的图形推导出来, 命题 "$\frac{1}{\pi}\arccos\left(\frac{1}{\sqrt{n}}\right)$ 是无理数" 等价于说通过 $\frac{1}{\sqrt{n}}$ 构造的等边的多边形永远不会封闭.

我们把证明 $A(n)$ 仅当 $n \in \{1,2,4\}$ 时是有理数留给读者作为练习. 那将要区分 $n=2^r$ 的情形和 n 不是 2 的幂的情形.

■ **证明.** 将三角学中的和角定理

$$\cos\alpha + \cos\beta = 2\cos\tfrac{\alpha+\beta}{2}\cos\tfrac{\alpha-\beta}{2}$$

用于 $\alpha=(k+1)\varphi$ 和 $\beta=(k-1)\varphi$, 我们得到

$$\cos(k+1)\varphi \; = \; 2\cos\varphi\cos k\varphi \; - \; \cos(k-1)\varphi. \tag{2}$$

对由 $\cos\varphi_n=\frac{1}{\sqrt{n}}$ 及 $0\leqslant\varphi_n\leqslant\pi$ 定义的角 $\varphi_n=\arccos\left(\frac{1}{\sqrt{n}}\right)$ 和非负整数 k, 这将导出表示

$$\cos k\varphi_n \; = \; \frac{A_k}{\sqrt{n}^k},$$

其中每个 A_k 都是不能被 n 整除的整数. 事实上, 取 $A_0=A_1=1$, 这个表示对 $k=0,1$ 时成立. 对 k 归纳, 利用 (2) 我们得到当 $k\geqslant 1$ 时有

$$\cos(k+1)\varphi_n \; = \; 2\frac{1}{\sqrt{n}}\frac{A_k}{\sqrt{n}^k} - \frac{A_{k-1}}{\sqrt{n}^{k-1}} \; = \; \frac{2A_k - nA_{k-1}}{\sqrt{n}^{k+1}}.$$

于是有 $A_{k+1}=2A_k-nA_{k-1}$. 若 $n\geqslant 3$ 是奇数, 且 A_k 不被 n 整除, 则 A_{k+1} 也不被 n 整除.

现在假设

$$A(n) \;=\; \frac{1}{\pi}\varphi_n \;=\; \frac{k}{\ell}$$

是有理数 ($k, \ell > 0$ 是整数). 那么 $\ell\varphi_n = k\pi$ 导致

$$\pm 1 \;=\; \cos k\pi \;=\; \frac{A_\ell}{\sqrt{n}^{\ell}}.$$

从而 $\sqrt{n}^{\ell} = \pm A_\ell$ 是整数, 又 $\ell \geqslant 2$, 故 $n \,|\, \sqrt{n}^{\ell}$. 由 $\sqrt{n}^{\ell} \,|\, A_\ell$ 我们得到 n 整除 A_ℓ, 矛盾. □

参考文献

[1] C. Hermite: *Sur la fonction exponentielle,* Comptes rendus de l'Académie des Sciences (Paris) **77** (1873), 18-24; Œuvres de Charles Hermite, Vol. III, Gauthier-Villars, Paris 1912, pp. 150-181.

[2] Y. Iwamoto: *A proof that π^2 is irrational,* J. Osaka Institute of Science and Technology **1** (1949), 147-148.

[3] J. F. Koksma: *On Niven's proof that π is irrational,* Nieuw Archief voor Wiskunde (2) **23** (1949), 39.

[4] J. Liouville: *Sur l'irrationalité du nombre* e = 2,718..., Journal de Mathématiques Pures et Appl. (1) **5** (1840), 192; *Addition*, 193-194.

[5] I. Niven: *A simple proof that π is irrational,* Bulletin Amer. Math. Soc. **53** (1947), 509.

三探 $\pi^2/6$　　第 7 章

我们知道无穷级数 $\sum_{n\geqslant 1}\frac{1}{n}$ 发散. 事实上, 在第 1 章我们已看到 $\sum_{p\in\mathbb{P}}\frac{1}{p}$ 也是发散的.

尽管如此, 平方的倒数之和收敛 (虽然收敛得很慢, 我们将看到), 而且收敛到一个有趣的数.



欧拉级数.

$$\sum_{n\geqslant 1}\frac{1}{n^2} \;=\; \frac{\pi^2}{6}.$$

这是 1734 年 Leonhard Euler 做出的一个经典、著名且重要的结果. 这个事实的一个重要解释是它导出了 Riemann zeta 函数的第一个非平凡值 $\zeta(2)$ (见后面的附录). 正如我们在第 6 章所看到的, 这个数值是无理数.

不仅这一结果在数学史上具有显赫的地位, 它的几个极其优美聪明的证明也拥有自己的历史. 对它们的发现与再发现的乐趣被很多人分享. 本章就介绍三个这样的证明.

1	$=$	1.000000
$1+\frac{1}{4}$	$=$	1.250000
$1+\frac{1}{4}+\frac{1}{9}$	$=$	1.361111
$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}$	$=$	1.423611
$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\frac{1}{25}$	$=$	1.463611
$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\frac{1}{25}+\frac{1}{36}$	$=$	1.491388
$\pi^2/6$	$=$	1.644934.

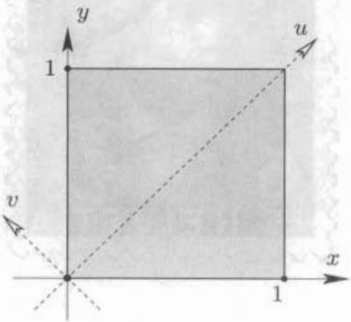
■ **证明.** 第一个证明出现在 1956 年 William J. LeVeque 的数论教科书里, 是一道练习题. 不过他说: "关于这道题目的来源我毫无所知, 但我确信它不是我的原创."

这个证明包含对重积分

$$I \;:=\; \int_0^1\!\!\int_0^1 \frac{1}{1-xy}\,dx\,dy$$

的两个不同的估计. 第一个, 把 $\frac{1}{1-xy}$ 展成几何级数, 把和式分解为乘积, 然后毫不费力地求积分:

$$\begin{aligned} I &= \int_0^1\int_0^1 \sum_{n\geqslant 0}(xy)^n\,dx\,dy = \sum_{n\geqslant 0}\int_0^1\int_0^1 x^n y^n\,dx\,dy \\ &= \sum_{n\geqslant 0}\left(\int_0^1 x^n dx\right)\left(\int_0^1 y^n dy\right) = \sum_{n\geqslant 0}\frac{1}{n+1}\,\frac{1}{n+1} \\ &= \sum_{n\geqslant 0}\frac{1}{(n+1)^2} = \sum_{n\geqslant 1}\frac{1}{n^2} = \zeta(2). \end{aligned}$$

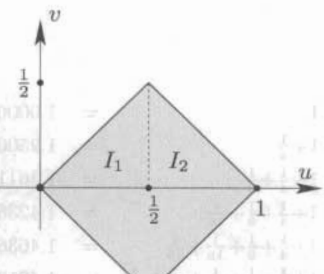


这个计算也说明 (在 $x = y = 1$ 处有一个极点的正函数) 二重积分是有限的. 注意, 从后往前看这个计算也是简单且直截了当的, 故对 $\zeta(2)$ 的估值把我们引向二重积分 I.

第二个计算 I 的方法来自坐标变换: 新坐标系由 $u := \frac{y+x}{2}$ $v := \frac{y-x}{2}$ 给出, 其定积分的定义域是一个边长为 $\frac{1}{2}\sqrt{2}$ 的正方形, 可以通过旋转旧的定义域 45° 再以 $\sqrt{2}$ 的比率缩小. 作代换 $x = u - v$ 和 $y = u + v$, 有

$$\frac{1}{1-xy} = \frac{1}{1-u^2+v^2}.$$

为转换积分, 并弥补变量替换将面积缩小一半的事实, 须将 $dx\,dy$ 替换为 $2\,du\,dv$ (此即变量替换的 Jacobi 行列式, 见下页边框). 新的积分定义域和积分函数都是关于 u- 轴对称的, 所以我们只须计算在上半平面积分的两倍 (又一个 2 出现在这!). 我们用最自然的方式把它分成两部分:



$$I = 4\int_0^{1/2}\left(\int_0^u \frac{dv}{1-u^2+v^2}\right)du + 4\int_{1/2}^1\left(\int_0^{1-u}\frac{dv}{1-u^2+v^2}\right)du.$$

由 $\displaystyle\int \frac{dx}{a^2+x^2} = \frac{1}{a}\arctan\frac{x}{a} + C$, 上式化为

$$\begin{aligned} I = &\ 4\int_0^{1/2}\frac{1}{\sqrt{1-u^2}}\arctan\left(\frac{u}{\sqrt{1-u^2}}\right)du \\ &+ 4\int_{1/2}^1 \frac{1}{\sqrt{1-u^2}}\arctan\left(\frac{1-u}{\sqrt{1-u^2}}\right)du. \end{aligned}$$

这两个积分可以通过代换 $u = \sin\theta$ 及 $u = \cos\theta$ 简化并最终计算出来. 但我们更直接地来做, 容易计算 $g(u) := \arctan\left(\frac{u}{\sqrt{1-u^2}}\right)$ 的导数是 $g'(u) = \frac{1}{\sqrt{1-u^2}}$, $h(u) := \arctan\left(\frac{1-u}{\sqrt{1-u^2}}\right) = \arctan\left(\sqrt{\frac{1-u}{1+u}}\right)$ 的导数是 $h'(u) = -\frac{1}{2}\frac{1}{\sqrt{1-u^2}}$. 所以我们可以用 $\int_a^b f'(x)f(x)dx =$

$\left[\frac{1}{2}f(x)^2\right]_a^b = \frac{1}{2}f(b)^2 - \frac{1}{2}f(a)^2$ 来得到

$$\begin{aligned} I &= 4\int_0^{1/2} g'(u)g(u)\,du + 4\int_{1/2}^1 -2h'(u)h(u)\,du \\ &= 2\Big[g(u)^2\Big]_0^{1/2} - 4\Big[h(u)^2\Big]_{1/2}^1 \\ &= 2g(\tfrac{1}{2})^2 - 2g(0)^2 - 4h(1)^2 + 4h(\tfrac{1}{2})^2 \\ &= 2\left(\tfrac{\pi}{6}\right)^2 - 0 - 0 + 4\left(\tfrac{\pi}{6}\right)^2 = \tfrac{\pi^2}{6}. \qquad \square \end{aligned}$$

以上的证明通过一个定积分来得到 Euler 级数的值, 仅仅是利用了一个很简单的坐标变换. 后来 Beukers, Calabi 与 Kolk 发现了同样类型的一个精巧证明, 却用到了一个全然非平凡的坐标转换. 那个证明的起始点在于将 $\sum_{n\geqslant 1}\frac{1}{n^2}$ 分拆成偶数项和奇数项. 显然偶数项的和 $\frac{1}{2^2}+\frac{1}{4^2}+\frac{1}{6^2}+\cdots=\sum_{k\geqslant 1}\frac{1}{(2k)^2}$ 是 $\frac{1}{4}\zeta(2)$, 所以奇数项的和 $\frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\cdots=\sum_{k\geqslant 0}\frac{1}{(2k+1)^2}$ 是 $\zeta(2)$ 的 3/4. 因此 Euler 级数等价于

$$\sum_{k\geqslant 0}\frac{1}{(2k+1)^2} = \frac{\pi^2}{8}.$$

■ **证明.** 如前, 表成二重积分, 即

$$J = \int_0^1\int_0^1 \frac{1}{1-x^2y^2}\,dx\,dy = \sum_{k\geqslant 0}\frac{1}{(2k+1)^2}.$$

故须计算 J. 为此, Beukers, Calabi 和 Kolk 提出了新的坐标

$$u := \arccos\sqrt{\frac{1-x^2}{1-x^2y^2}} \qquad v := \arccos\sqrt{\frac{1-y^2}{1-x^2y^2}}.$$

计算重积分可以丢掉边界, 仅考虑在区间 $0<x<1$ 和 $0<y<1$ 中的 x, y. 这时 u, v 在三角形 $u>0, v>0, u+v<\pi/2$ 中. 显然这个坐标变换可逆, 这用到替换

$$x = \frac{\sin u}{\cos v} \quad \text{及} \quad y = \frac{\sin v}{\cos u}.$$

从而可见以上的公式在单位正方形 $S=\{(x,y): 0\leqslant x, y\leqslant 1\}$ 的内部和三角形 $T=\{(u,v): u,v\geqslant 0,\ u+v\leqslant\pi/2\}$ 的内部之间定义了一个双射的坐标变换.

替换公式

为计算二重积分

$$I = \int_S f(x,y)\,dx\,dy,$$

若 $(u,v)\in T$ 到 $(x,y)\in S$ 的对应是双射且连续可微, 就可以做变量替换

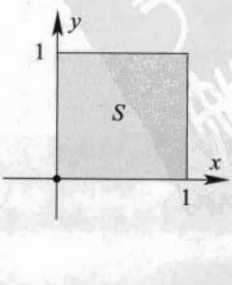
$$x = x(u,v) \quad y = y(u,v).$$

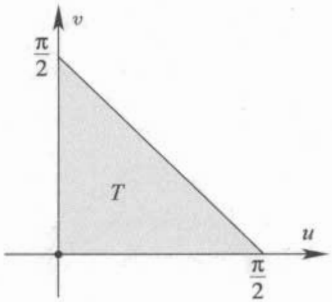
则 I 等于

$$\int_T f(x(u,v),y(u,v))\left|\frac{d(x,y)}{d(u,v)}\right|du\,dv,$$

其中 $\frac{d(x,y)}{d(u,v)}$ 是 Jacobi 行列式:

$$\frac{d(x,y)}{d(u,v)} = \det\begin{pmatrix} \frac{dx}{du} & \frac{dx}{dv} \\ \frac{dy}{du} & \frac{dy}{dv} \end{pmatrix}.$$





现在我们要计算坐标转换的 Jacobi 行列式, 奇妙的是它就是

$$\det\begin{pmatrix} \frac{\cos u}{\cos v} & \frac{\sin u \sin v}{\cos^2 v} \\ \frac{\sin u \sin v}{\cos^2 u} & \frac{\cos v}{\cos u} \end{pmatrix} = 1 - \frac{\sin^2 u \sin^2 v}{\cos^2 u \cos^2 v} = 1 - x^2 y^2.$$

这样我们想要计算的积分变成了

$$J = \int_0^{\pi/2} \int_0^{\pi/2-u} 1 \, du \, dv.$$

它正是三角形 T 的面积 $\frac{1}{2}(\frac{\pi}{2})^2 = \frac{\pi^2}{8}$. □

漂亮, 甚至更过之, 对所有的 $k \geqslant 1$, 证明中同样的方法还可推广到通过计算 $2k$- 重的定积分来得到 $\zeta(2k)$. 我们请读者看 Beuker, Calabi 和 Kolk 的文章, 以及第 20 章: 在那里我们从其他的途径达到同一个目的, 用到 Herglotz 的技巧和 Euler 的原始方法.

在这两个坐标变换的证明之后, 我们介绍另一个彻底不同且完全初等的对 $\sum_{n\geqslant 1} \frac{1}{n^2} = \frac{\pi^2}{6}$ 的证明, 这诱惑难以抗拒. 它最初出现在孪生兄弟 Akiva 和 Isaak Yaglom 著的习题集的一系列练习里面, 该俄文书于 1954 年问世. 这个美丽证明的其他版本被后人多次重新发现和描述, 这包括 F. Holme (1970), I. Papadimitriou (1973), 和将之归功于 John Scholes的 Ransford (1982).

■ **证明.** 第一步是在 (平方了的) 余切函数值之间建立一个重要关系: 对 $m \geqslant 1$, 有

$$\cot^2\left(\tfrac{\pi}{2m+1}\right) + \cot^2\left(\tfrac{2\pi}{2m+1}\right) + \cdots + \cot^2\left(\tfrac{m\pi}{2m+1}\right) = \tfrac{2m(2m-1)}{6}. \quad (1)$$

当 $m = 1, 2, 3$ 时我们得到
$\cot^2 \frac{\pi}{3} = \frac{1}{3}$
$\cot^2 \frac{\pi}{5} + \cot^2 \frac{2\pi}{5} = 2$
$\cot^2 \frac{\pi}{7} + \cot^2 \frac{2\pi}{7} + \cot^2 \frac{3\pi}{7} = 5$

为验证这个关系, 我们从

$$\cos nx + i \sin nx = (\cos x + i \sin x)^n$$

开始, 取虚部, 得

$$\sin nx = \binom{n}{1} \sin x \cos^{n-1} x - \binom{n}{3} \sin^3 x \cos^{n-3} x \pm \cdots \quad (2)$$

令 $n = 2m+1$, 而对 x 我们将要考虑 m 个不同的值 $x = \frac{r\pi}{2m+1}$, 其中 $r = 1, 2, \cdots, m$. 对每个这样的值我们有 $nx = r\pi$, 于是 $\sin nx = 0$, 而 $0 < x < \frac{\pi}{2}$ 表明对 $\sin x$ 我们得到了 m 个互异的正值.

特别地, 可以用 $\sin^n x$ 分别除 (2) 的两边得到

$$0 = \binom{n}{1} \cot^{n-1} x - \binom{n}{3} \cot^{n-3} x \pm \cdots,$$

亦即对 x 所取的这 m 个值中的每一个都有

$$0 = \binom{2m+1}{1}\cot^{2m} x - \binom{2m+1}{3}\cot^{2m-2} x \pm \cdots.$$

因此以下的 m 次多项式

$$p(t) := \binom{2m+1}{1}t^m - \binom{2m+1}{3}t^{m-1} \pm \cdots + (-1)^m\binom{2m+1}{2m+1}$$

有 m 个互异的根

$$a_r = \cot^2\left(\tfrac{r\pi}{2m+1}\right), \quad r = 1, 2, \cdots, m.$$

从而这个多项式正是

$$p(t) = \binom{2m+1}{1}\left(t - \cot^2\left(\tfrac{\pi}{2m+1}\right)\right)\cdot \cdots \cdot \left(t - \cot^2\left(\tfrac{m\pi}{2m+1}\right)\right).$$

与 $p(t)$ 的 t^{m-1} 项系数作比较得到诸根的和即

$$a_1 + \cdots + a_r = \frac{\binom{2m+1}{3}}{\binom{2m+1}{1}} = \frac{2m(2m-1)}{6},$$

比较系数:
若 $p(t) = c(t-a_1)\cdots(t-a_m)$,
则 t^{m-1} 的系数即
$-c(a_1 + \cdots + a_m)$.

这样我们证明了 (1).

我们还需要关于余割函数 $\csc x = \frac{1}{\sin x}$ 的一个同样类型的等式,

$$\csc^2\left(\tfrac{\pi}{2m+1}\right) + \csc^2\left(\tfrac{2\pi}{2m+1}\right) + \cdots + \csc^2\left(\tfrac{m\pi}{2m+1}\right) = \frac{2m(2m+2)}{6}. \quad (3)$$

但

$$\csc^2 x = \frac{1}{\sin^2 x} = \frac{\cos^2 x + \sin^2 x}{\sin^2 x} = \cot^2 x + 1,$$

故只要将 (1) 的两端同时加 m 就得到了 (3).

现在舞台搭好了, 各就其位. 在区间 $0 < y < \frac{\pi}{2}$ 内有

$$0 < \sin y < y < \tan y,$$

$0 < a < b < c$ 表明 $0 < \frac{1}{c} < \frac{1}{b} < \frac{1}{a}$

从而

$$0 < \cot y < \frac{1}{y} < \csc y.$$

这表明

$$\cot^2 y < \frac{1}{y^2} < \csc^2 y.$$

现在看这个双向不等式, 代入 x 的那 m 个互异的值, 再把结果加起来. 左端用 (1), 右端用 (3), 得到

$$\frac{2m(2m-1)}{6} \;<\; \left(\frac{2m+1}{\pi}\right)^2+\left(\frac{2m+1}{2\pi}\right)^2+\cdots+\left(\frac{2m+1}{m\pi}\right)^2 \;<\; \frac{2m(2m+2)}{6},$$

亦即,

$$\frac{\pi^2}{6}\frac{2m}{2m+1}\frac{2m-1}{2m+1} \;<\; \frac{1}{1^2}+\frac{1}{2^2}+\cdots+\frac{1}{m^2} \;<\; \frac{\pi^2}{6}\frac{2m}{2m+1}\frac{2m+2}{2m+1}.$$

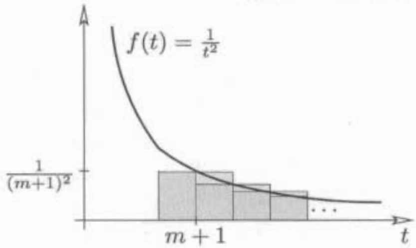
当 $m \longrightarrow \infty$ 时, 左右两端都收敛到 $\pi^2/6$: 证毕. □

那么 $\sum \frac{1}{n^2}$ 收敛到 $\pi^2/6$ 有多快呢? 为此需要估计差

$$\frac{\pi^2}{6}-\sum_{n=1}^{m}\frac{1}{n^2} \;=\; \sum_{n=m+1}^{\infty}\frac{1}{n^2}.$$

利用我们在第 2 章的附录中回顾过的 "与定积分比较" 技巧, 这将很容易. 推导得 "剩余部分和" 的上界

$$\sum_{n=m+1}^{\infty}\frac{1}{n^2} \;<\int_m^{\infty}\frac{1}{t^2}dt = \;\frac{1}{m}$$



和下界

$$\sum_{n=m+1}^{\infty}\frac{1}{n^2} \;>\; \int_{m+1}^{\infty}\frac{1}{t^2}dt \;=\; \frac{1}{m+1}.$$

如果想做略为精细一点的估计, 还可由 $f(t)=\frac{1}{t^2}$ 是凸函数, 得到

$$\sum_{n=m+1}^{\infty}\frac{1}{n^2} > \int_{m+\frac{1}{2}}^{\infty}\frac{1}{t^2}dt \;=\; \frac{1}{m+\frac{1}{2}}.$$

这说明我们的级数收敛得不太好; 对前 1000 项求和, 小数点后第三位还会有误差, 而如果对前一百万项求和, $m=1000000$, 那我们预期在第六位小数点处有误差, 的确是这样. 尽管如此, 有一个很大的意外: 精确到 45 位,

$$\begin{aligned}\pi^2/6 \;&=\; 1.644934066848226436472415166646025189218949901,\\ \sum_{n=1}^{10^6}\frac{1}{n^2} \;&=\; 1.644933066848726436305748499979391855885616544.\end{aligned}$$

所以小数点后第六位错了 (小了 1), 但是接下去的六个数准确无误! 再接下去的数字是错的 (大了 5), 然后又有五个数是对的. 这个令人惊奇的事实是由 Colorado Springs 的 Roy D. North 在 1988 年发现的.

(1982 年, 受制于当时不足的计算能力, 英格兰 Bucks 郡 Amersham 的教师 Martin R. Powell 未能注意到事实的全貌.) 如此奇特, 不可能完全属于巧合 …… 观察误差项, 仍取 45 位,

$$\sum_{n=10^6+1}^{\infty} \frac{1}{n^2} = 0.000000999999500000166666666666633333333333357,$$

揭示了这明显存在某种规律. 也许可将最后一个数写成

$$+10^{-6} - \tfrac{1}{2}10^{-12} + \tfrac{1}{6}10^{-18} - \tfrac{1}{30}10^{-30} + \tfrac{1}{42}10^{-42} + \cdots$$

则 10^{-6i} 项的系数 $(1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, \frac{1}{42})$ 构成了 *Bernoulli 数* 序列的起始部分, 在第 20 章还会遇到它们. 请读者看 Borwein, Borwein & Dilcher 的文章 [3], 那里有更多这样意外的 "巧合", 包括证明.

附录: Riemann zeta 函数

对实数 $s > 1$, *Riemann zeta 函数* $\zeta(s)$ 的定义为

$$\zeta(s) := \sum_{n \geqslant 1} \frac{1}{n^s}.$$

我们对 H_n 的估计 (见第 2 章) 表明级数 $\zeta(1)$ 发散, 而对实数 $s > 1$ 它确实收敛. Zeta 函数在整个复平面有着经典的连续 (在 $s = 1$ 处有一个简单的极点) 并可以由幂级数构造出来. 所得的复函数在素数理论中是至关重要的. 让我们介绍三个不同的关联:

(1) 著名的等式

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}$$

属于 Euler. 它蕴含了每个自然数有唯一 (!) 素数分解的基本事实; 由这个事实, Euler 的等式就是下面几何级数展开的自然推论了:

$$\frac{1}{1 - p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots$$

(2) Zeta 函数复零点的位置是 "Riemann 猜想" 的主题, 是整个数学领域中最著名和重要的待解决问题之一. 该猜想断言 zeta 函数的所有非平凡零点 $s \in \mathbb{C}$ 满足 $\mathrm{Re}(s) = \frac{1}{2}$. (Zeta 函数在所有负的偶数点处为零, 这些点被称为 "平凡零点".)

最近, Jeff Lagarias 出人意料地证明了 Riemann 猜想等价于以下的初等命题: 对所有的 $n \geqslant 1$,

$$\sum_{d \mid n} d \ \leqslant \ H_n \ + \ \exp(H_n) \log(H_n),$$

等式成立仅当 $n = 1$, 这里 H_n 还是第 2 章附录中的调和数.

(3) 以下事实久已为人所知: 若 s 是 $\geqslant 2$ 的偶数, 则 $\zeta(s)$ 是 π^s 的有理数倍, 所以是无理数; 见第 20 章. 对比之下, 直到 1979 年, 才由 Roger Apéry 证明 $\zeta(3)$ 的无理性. 尽管人们付出了相当大的努力, 关于 $\zeta(s)$ 在其他奇整数 $s = 2t + 1 \geqslant 5$ 时的类似结果仍旧颇为欠缺. 最近, Keith Ball 和 Tanguy Rivoal 证明了有无穷多个 $\zeta(2t+1)$ 是无理的. 然而, 我们还不知道对任何一个奇的 $s \geqslant 5$, $\zeta(s)$ 是无理数. Wadim Zudilin 证明了 $\zeta(5)$, $\zeta(7)$, $\zeta(9)$ 和 $\zeta(11)$ 中至少有一个是无理的. 请看 Fischler 的精彩综述 [4].

参考文献

[1] K. Ball & T. Rivoal: *Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs,* Inventiones math. **146** (2001), 193-207.

[2] F. Beukers, J. A. C. Kolk & E. Calabi: *Sums of generalized harmonic series and volumes,* Nieuw Archief voor Wiskunde (4) **11** (1993), 217-224.

[3] J. M. Borwein, P. B. Borwein & K. Dilcher: *Pi, Euler numbers, and asymptotic expansions,* Amer. Math. Monthly **96** (1989), 681-687.

[4] S. Fischler: *Irrationalité de valeurs de zêta (d'après Apéry, Rivoal, $\cdots$),* Bourbaki Seminar, No. 910, November 2002; *Astérisque* **294** (2004), 27-62.

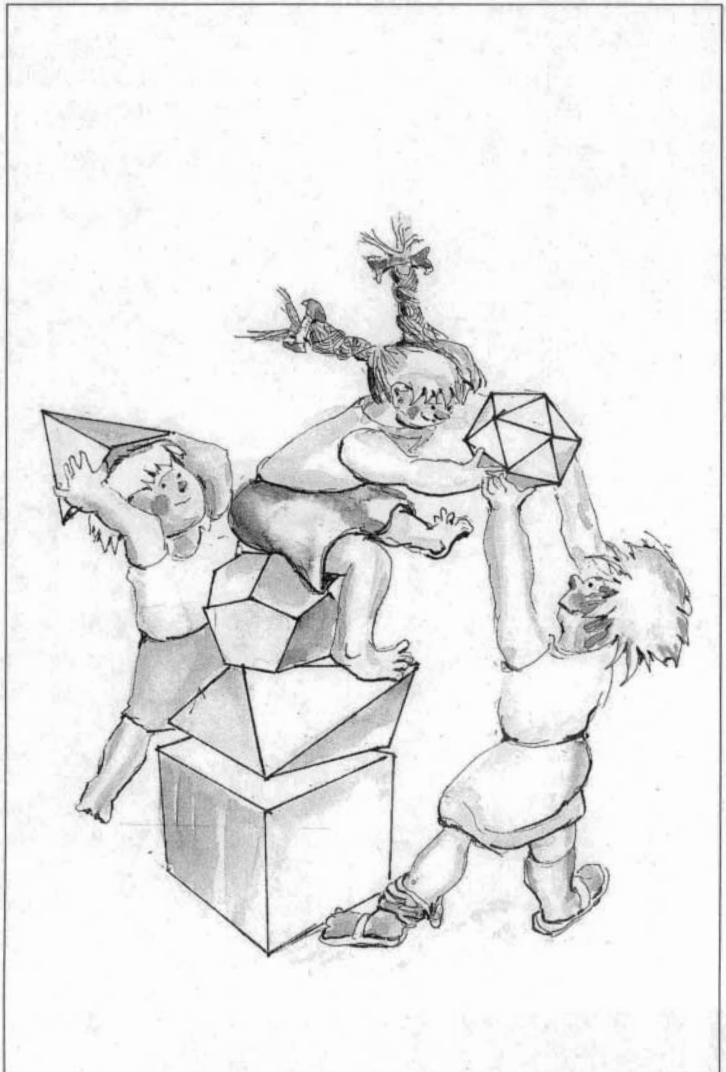
[5] J. C. Lagarias: *An elementary problem equivalent to the Riemann hypothesis,* Amer. Math. Monthly **109** (2002), 534-543.

[6] W. J. LeVeque: *Topics in Number Theory,* Vol. I, Addison-Wesley, Reading MA 1956.

[7] A. M. Yaglom & I. M. Yaglom: *Challenging mathematical problems with elementary solutions,* Vol. II, Holden-Day, Inc., San Francisco, CA 1967.

[8] W. Zudilin: *Arithmetic of linear forms involving odd zeta values,* J. Théorie Nombres Bordeaux **16** (2004), 251-291.

几　何



Plato 多面体 — 小孩子的游戏

几何

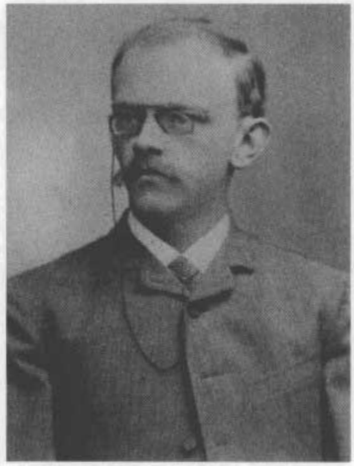
Plato 多面体——小孩子的游戏

Hilbert 第三问题: 多面体的分解

第 8 章

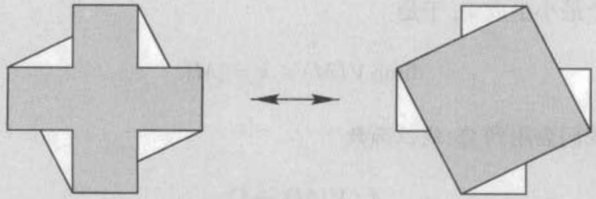
1900 年的巴黎国际数学家大会上, David Hilbert 在他的著名演讲中提出了如下问题作为他 23 个问题中的第 3 个:

> 找出两个具有相同底面积和高的四面体, 它们不能被分割成两组对应全等的四面体, 通过任何方式各自拼接若干个对应全等的四面体后得到的多面体也不能被切割成两组对应全等的四面体.

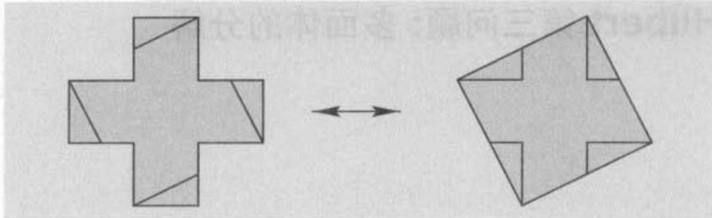


David Hilbert

这个问题可以追溯到Carl Friedrich Gauss于 1844 年所写的两封信 (被收集在 1900 年出版的 Gauss 全集中). 如果任意两个具有相同体积的四面体可以被切割成若干个对应全等的四面体, 则它可为Euclid的定理 XII.5 提供一个 "初等" 证明, 定理 XII.5 说两个具有相同底和高的锥体体积相同. 从而, 它也提供了一个多面体体积的初等定义 (并非基于分析, 从而不依赖于连续性讨论). 一个相似的命题在平面几何中是成立的: Bolyai-Gerwien 定理 [1, 2.7 节] 认为平面多边形既是可全等分割的 (可被切割成对应全等的三角形) 也是可全等拼接的 (可通过拼接对应全等的三角形成为全等的) 当且仅当它们的面积相等.



这个十字架与具有相同面积的正方形是可全等拼接的



它们也是可全等分割的.

正如我们在他的第三问题中所看到的, Hilbert确实预料到在三维的情形没有类似的定理. 他是对的. 事实上, 这个问题被Hilbert的学生Max Dehn在两篇论文中完全解决了: 在 1900 年的第一篇论文中他找到了非可全等分割的具有相等底面积和高的四面体; 在 1902 年的第二篇论文中他还阐述了可全等拼接的条件. 然而, Dehn的论文不容易读懂, 还得花很大力气鉴定他是否落入其他人曾经掉进去过的小陷阱中: Bricard (1896 年) 和Meschkowski (1960 年)分别给出过非常优雅却不幸是错误的证明, 可能还有其他人也如此. 幸运的是, Dehn 的证明被重新整理并改进了, 结合V. F. Kagan (1903/1930 年), Hugo Hadwiger (1949/1954 年) 和Vladimir G. Boltjanskii的努力, 我们现在有了下面给出的这个天书证明 (多面体的基本知识参见本章附录).

(1) 一点线性代数的知识

对每个有限实数集合 $M=\{m_1,\cdots,m_k\}\subseteq\mathbb{R}$, 我们定义 $V(M)$ 为 M 中元素的所有有理系数线性组合所构成的集合, 即

$$V(M):=\Big\{\sum_{i=1}^{k}q_im_i : q_i\in\mathbb{Q}\Big\}\subseteq\mathbb{R}.$$

首先观察到 (平凡但是重要的) $V(M)$ 是有理数域 $\mathbb{Q}$ 上的有限维向量空间. 事实上, $V(M)$ 在加法和有理数乘法下显然是封闭的, $\mathbb{R}$ 的数域公理保证了 $V(M)$ 是一个向量空间. $V(M)$ 的维数就是它的最小生成集的元素个数. 由定义 M 生成了 $V(M)$. 可见 M 包含了一个最小生成集, 于是

$$\dim_{\mathbb{Q}}V(M)\leqslant k=|M|.$$

下面我们会用到 $\mathbb{Q}$- 线性函数

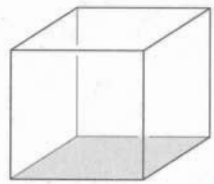
$$f:V(M)\to\mathbb{Q},$$

这里我们把它理解成 $\mathbb{Q}$- 向量空间的线性映射. 它的关键性质是如果 $\sum_{i=1}^{k} q_i m_i = 0, q_i \in \mathbb{Q}$, 则必有 $\sum_{i=1}^{k} q_i f(m_i) = f(0) = 0$. 下面这个简单的引理可使情况更进一步.

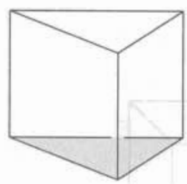
引理. *对任意的有限子集 $M \subseteq M' \subseteq \mathbb{R}$, $\mathbb{Q}$- 向量空间 $V(M)$ 是 $\mathbb{Q}$- 向量空间 $V(M')$ 的子空间. 因此, 如果 $f : V(M) \to \mathbb{Q}$ 是一个 $\mathbb{Q}$- 线性函数, 那么 f 可以扩展成 $\mathbb{Q}$- 线性函数 $f' : V(M') \to \mathbb{Q}$ 使得对任意 $m \in M$, 有 $f'(m) = f(m)$.*

■ **证明**. 任意一个 $\mathbb{Q}$- 线性函数 $V(M) \to \mathbb{Q}$ 被它在 $V(M)$ 的一个 $\mathbb{Q}$- 基上的值完全决定. 既然 $V(M)$ 的每个基都可以扩展成 $V(M')$ 的基, 这便推出引理. □

(2) Dehn 不变量



$M_C = \{\frac{\pi}{2}, \pi\}$



$M_Q = \{\frac{\pi}{3}, \frac{\pi}{2}, \pi\}$

对于一个三维多面体 P, 令 M_P 表示所有相邻面之间的夹角 (二面角) 以及 π 组成的集合. 例如对于正方体 C, 我们有 $M_C = \{\frac{\pi}{2}, \pi\}$, 而对于底面是等边三角形的正棱柱体 Q, 我们有 $M_Q = \{\frac{\pi}{3}, \frac{\pi}{2}, \pi\}$.

给定任何包含 M_P 的有限集合 $M \subseteq \mathbb{R}$ 以及任何满足 $f(\pi) = 0$ 的 $\mathbb{Q}$- 线性函数

$$f : V(M) \to \mathbb{Q},$$

我们定义 P 的 (关于 f 的) *Dehn* 不变量为实数值

$$D_f(P) := \sum_{e \in P} \ell(e) \cdot f(\alpha(e)),$$

其中 $\ell(e)$ 表示边 e 的长度, $\alpha(e)$ 表示相交于 e 的二个面的夹角.

后面我们将计算几类不同的 Dehn 不变量. 现在我们只需注意到对每个 $\mathbb{Q}$- 线性函数 f 一定有 $f\left(\frac{\pi}{2}\right) = \frac{1}{2} f(\pi) = 0$. 从而

$$D_f(C) = 0,$$

也就是说, 立方体的关于任意 f 的 Dehn 不变量是 0.

(3) Dehn-Hadwiger 定理

如上所述, 我们称多面体 P 和 Q 为可全等分割的, 如果它们可以被分割成有限个多面体 $P_1, \cdots, P_n$ 和 $Q_1, \cdots, Q_n$ 使得对所有指标 i $(1 \leqslant i \leqslant n)$, P_i 和 Q_i 都是全等的. 两个多面体是可全等拼接的, 如果存在多面体 $P_1, \cdots, P_m$ 和 $Q_1, \cdots, Q_m$, 其中 P_i 的内部彼

此不交, 也与 P 的内部不交, Q_i 与 Q 也如此, 使得对所有指标 i, P_i 和 Q_i 都是全等的, 并且 $\widetilde{P} := P \cup P_1 \cup P_2 \cup \cdots \cup P_m$ 和 $\widetilde{Q} := Q \cup Q_1 \cup Q_2 \cup \cdots \cup Q_m$ 是可全等分割的. 1844 年Gerling得到的一个定理表明这里的全等与是否允许反射无关.

显然, 可全等分割的多面体是可全等拼接的, 但反之是还不明显的. 接下来的Hadwiger 定理 (Boltjanskii 的版本) 为我们找到Hilbert第三问题中的等体积, 但不可全等分割, 从而也不可全等拼接的四面体提供了工具.

定理. 设 P 和 Q 是两个多面体, $\alpha_1, \cdots, \alpha_p$ 和 $\beta_1, \cdots, \beta_q$ 分别表示它们的二面角, M 为一个由实数组成的有限集合且满足

$$\{\alpha_1, \cdots, \alpha_p, \beta_1, \cdots, \beta_q, \pi\} \subseteq M.$$

如果 $f : V(M) \to \mathbb{Q}$ 是一个满足 $f(\pi) = 0$ 的 $\mathbb{Q}$- 线性函数, 并且

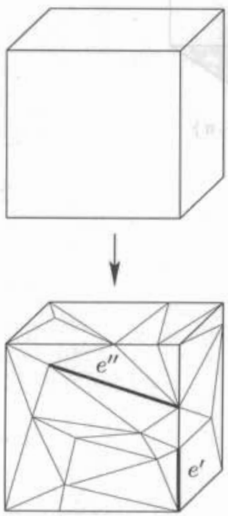
$$D_f(P) \neq D_f(Q),$$

那么 P 和 Q 不是可全等拼接的.

■ **证明.** 证明由两部分组成.

(1) 如果多面体 P 可以被切割成有限多个多面体 $P_1, \cdots, P_n$, 并且如果 $P_1, \cdots, P_n$ 的所有二面角被包含在集合 M 内, 则对任意的 $\mathbb{Q}$- 线性函数 $f : V(M) \to \mathbb{Q}$, Dehn 不变量可加起来:

$$D_f(P) = D_f(P_1) + \cdots + D_f(P_n).$$



为了证明这个等式, 我们首先给多面体的一条边 e 的任意一部分 e' 结合一个质量:

$$m_f(e') := \ell(e')\, f(\alpha(e')),$$

即 e' 的长度乘以它的二面角的 f- 值.

现在如果 P 被切割成 $P_1, \cdots, P_n$, 考虑这些分块 P_i 的所有边组成的集合. 如果边 e' 是 P 的某条边的一部分, 我们可以看到, 所有包含边 e' 的多面体在 e' 的二面角的和就是 P 在 e' 的二面角的和, 从而 e' 在它们中的质量的和即为 e' 在 P 中的质量.

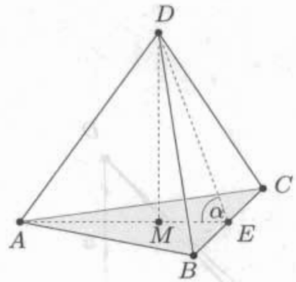
对于任何其他的包含在 P 的某个面或内部上的 P_i 的边 e'' 的二面角的和为 π 或 2π, 所以二面角的 f- 值的和分别为 $f(\pi) = 0$ 或 $f(2\pi) = 0$. 从而加在 P 的这些边上的质量的和为 0.

(2) 假设 P 和 Q 是可全等拼接的, 我们可以把集合 M 扩充为更大的集合 M', 保留所有原来分块中出现的二面角. 因为我们只考虑有限分割, M' 是有限的. 那么上面的引理允许我们拓展 f 到 $f': V(M') \to \mathbb{Q}$, 结合 (1) 得到

$$D_{f'}(P) + D_{f'}(P_1) + \cdots + D_{f'}(P_m)$$
$$= D_{f'}(Q) + D_{f'}(Q_1) + \cdots + D_{f'}(Q_m),$$

其中 P_i 和 Q_i 全等推出 $D_{f'}(P_i) = D_{f'}(Q_i)$. 从而我们得到 $D_f(P) = D_f(Q)$, 矛盾! □

例 1. T_0 表示一个边长为 ℓ 的正四面体, 我们由简图计算它的二面角. 底面三角形的中点 M 将高 AE 分成长度比为 1:2 的两条线段, 再由 $|AE| = |DE|$, 我们得到 $\cos\alpha = \frac{1}{3}$, 从而



$$\alpha = \arccos\tfrac{1}{3}.$$

令 $M := \{\alpha, \pi\}$, 我们注意到

$$\frac{\alpha}{\pi} = \frac{1}{\pi}\arccos\tfrac{1}{3}$$

是无理数 (在第 6 章定理 3 中取 $n = 9$). 从而 $\mathbb{Q}$- 向量空间 $V(M)$ 是以 M 为基的一个二维向量空间, 并且存在 $\mathbb{Q}$ - 线性函数 $f: V(M) \to \mathbb{Q}$ 满足

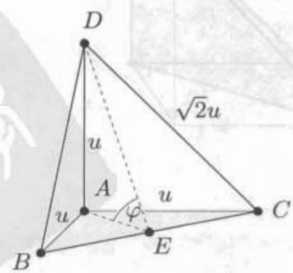
$$f(\alpha) := 1,\ f(\pi) := 0.$$

对于这个 f 我们有

$$D_f(T_0) = 6\ell f(\alpha) = 6\ell \neq 0,$$

所以体积相同的正四面体和立方体不能全等分割或全等拼接, 因为立方体的 Dehn 不变量对任何 f 均为 0.

例 2. T_1 是一个由三条长为 u 的互相垂直的边 AB, AC, AD 生成的四面体. 这个四面体有三个直角二面角, 还有三个大小为 φ 的二面角, 我们由图计算得到



$$\cos\varphi = \frac{|AE|}{|DE|} = \frac{\frac{1}{2}\sqrt{2}u}{\frac{1}{2}\sqrt{3}\,\sqrt{2}u} = \frac{1}{\sqrt{3}},$$

所以

$$\varphi = \arccos\frac{1}{\sqrt{3}}.$$

对于 $M := \{\frac{\pi}{2}, \arccos\frac{1}{\sqrt{3}}, \pi\}$, $\mathbb{Q}$- 向量空间 $V(M)$ 是二维的. 事实上, π 和 $\frac{\pi}{2}$ 是有理线性相关的, 所以

$$V(M) = V\big(\{\arccos\frac{1}{\sqrt{3}}, \pi\}\big).$$

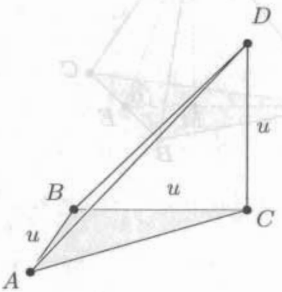
另一方面, $\arccos\frac{1}{\sqrt{3}}$ 和 π 不是有理线性相关的 (第 6 章定理 3 中取 $n = 3$, 我们得到 $\frac{1}{\pi}\arccos\frac{1}{\sqrt{3}}$ 是无理数). 从而我们可以构造一个 $\mathbb{Q}$- 线性函数 f 满足

$$f(\pi) := 0 \quad 和 \quad f\big(\arccos\tfrac{1}{\sqrt{3}}\big) := 1,$$

从定义得到 $f(\frac{\pi}{2}) = 0$ 并且因此

$$D_f(T_1) \ = \ 3uf\big(\tfrac{\pi}{2}\big) + 3(\sqrt{2}u)f\big(\arccos\tfrac{1}{\sqrt{3}}\big) \ = \ 3\sqrt{2}u \ \neq \ 0.$$

这证明了 T_1 和体积相同的立方体 C 不能全等分割, 也不能全等拼接, 因为 $D_f(C) = 0$ 对所有的 f 成立.



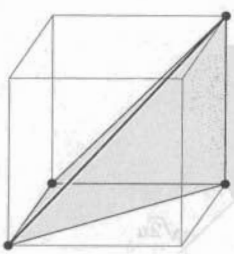
例 3. 令 T_2 是有三条互相垂直的边 AB, BC 和 CD 的四面体. AB, BC, CD 边长都为 u.

我们不必计算这个四面体的二面角 (它们是 $\pi/2$, $\pi/3$ 和 $\pi/4$), 而是通过利用边与面的中点以及中心指出: 一个边长为 u 的立方体可以分解成 6 个这类的四面体 (三个全等, 另三个为镜像).

所有这些全等的立方体与镜像有相同的 Dehn 不变量. 因此对每个符合定义的 f 都可得到

$$D_f(T_2) = \frac{1}{6}D_f(C) = 0.$$

所以这个四面体的所有 Dehn 不变量都消失了! 这就解决了 Hilbert 的第三问题, 因为之前我们构造了另一个等底等高的四面体 T_1 满足 $D_f(T_1) \neq 0$. 由 Dehn-Hadwiger 定理, T_1 和 T_2 不能全等分割, 也不能全等拼接.



附录: 多胞体和多面体

一个 $\mathbb{R}^d$ 中的凸多胞体是一个有限集 $S = \{s_1, \cdots, s_n\}$ 的凸包, 即

$$P \ = \ \text{conv}(S) \ := \Big\{\sum_{i=1}^{n}\lambda_i s_i : \lambda_i \geqslant 0, \ \sum_{i=1}^{n}\lambda_i = 1\Big\}.$$

事实上多胞体是我们熟悉的物体, 主要的例子有凸多边形 (二维的凸多胞体) 和凸多面体 (三维的凸多胞体).

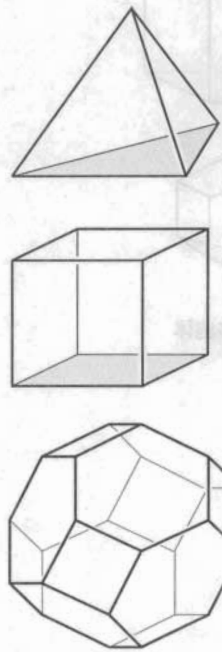
有几类多面体可以比较自然地推广到高维的情形. 例如, 如果集合 S 是仿射独立的, 基数是 $d+1$, 那么 S 的凸包是一个 d 维的单纯形 (d- 单纯形). $d=2$ 的情况得到一个三角形, $d=3$ 时得到一个四面体. 类似地, 正方形和立方体是 d- 立方体的特殊情形, 例如单位 d- 立方体 $C_d=[0,1]^d \subseteq \mathbb{R}^d$.

一般的多胞体由有限个凸多胞体拼接而成. 在这本书里非凸多面体将在第 12 章中有关 Cauchy 刚性定理的地方出现, 非凸多胞体将在第 11 章中有关 Pick 定理的地方出现, 并在第 31 章讨论关于美术馆的定理时再次出现.

凸多胞体可以等价地定义为有限线性不等式组的带边界解集. 从而任何凸多胞体 $P \subseteq \mathbb{R}^d$ 都可以表示成形式

$$P=\{\boldsymbol{x} \in \mathbb{R}^d : A\boldsymbol{x} \leqslant \boldsymbol{b}\},$$

其中 $A \in \mathbb{R}^{m\times d}$, 向量 $\boldsymbol{b} \in \mathbb{R}^m$. 也就是说, P 是 m 个线性不等式 $\boldsymbol{a}_i^T\boldsymbol{x} \leqslant b_i$ 的解集, 其中 $\boldsymbol{a}_i^T$ 是 A 的第 i 行. 反之, 每个这样的不等式组的带边界解集是一个凸多胞体, 从而可以表示成有限点集的凸包.



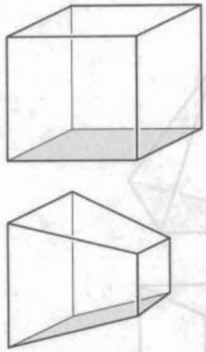
一些熟悉的凸多胞体: 四面体, 立方体, Permutahedron

对于多边形和多面体, 我们熟悉它们的顶点、边和面的概念. 高维凸多胞体的面可定义如下: P 的一个面是 P 的一个子集 $P\cap\{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{a}^T\boldsymbol{x}=b\}$, 其中 $\boldsymbol{a}^T\boldsymbol{x} \leqslant b$ 是对所有 $\boldsymbol{x} \in P$ 都满足的线性不等式之一.

多胞体的每个面本身也都是多胞体. 凸多胞体的顶点集 V(所有 0 维面组成的集合) 是使得 $\operatorname{conv}(V)=P$ 成立的在包含意义下的最小集合. 假设 $P \subseteq \mathbb{R}^d$ 是一个 d 维凸多胞体, 则 P 的面 ($(d-1)$ 维面) 是满足下面条件的最小超平面集合: 这些超平面决定的包含 P 的半空间的交就是 P. 特别地, 我们将要用到以下事实: 设 F 是 P 的一个面, 用 H_F 表示 F 决定的超平面, H_F^+ 和 H_F^- 是以 H_F 为边界的两个闭的半空间. 则其中一个半空间包含 P(同时另一个不包含 P).

凸多胞体 P 的图 $G(P)$ 由顶点集 V 和边 (一维的面) 集 E 组成. 如果 P 是三维的, 那么这个图是平面图, 并且有著名的 "欧拉公式" (见第 11 章).

对于两个多胞体 $P, P' \subseteq \mathbb{R}^d$, 如果存在保长的仿射映射将 P 映射到 P', 则称 P,P' 是全等的. 这样的映射也许会改变空间的定向, 如 P 在某个超平面的反射把 P 映到它的镜像. 如果存在一个双射使得 P 的面对应到 P' 的面保持维数和包含关系不变, 那么称它们



组合等价的多胞体

为组合等价的. 组合等价的概念远弱于全等的概念: 如图显示的一个单位立方体和一个 "斜" 立方体是组合等价的 (从而我们可以把它们都称为立方体), 但它们显然不是全等的.

一个多胞体 (或更广泛地, 对 $\mathbb{R}^d$ 的任意一个子集) 称作是中心对称的, 如果存在一个点 $\boldsymbol{x}_0 \in \mathbb{R}^d$, 使得

$$\boldsymbol{x}_0 + \boldsymbol{x} \in P \iff \boldsymbol{x}_0 - \boldsymbol{x} \in P.$$

这时我们称 x_0 是 P 的中心.

参考文献

[1] V. G. Boltjanskii: *Hilbert's Third Problem,* V. H. Winston & Sons (Halsted Press, John Wiley & Sons), Washington DC 1978.

[2] M. Dehn: *Ueber raumgleiche Polyeder,* Nachrichten von der Königl. Gesellschaft der Wissenschaften, Mathematisch-physikalische Klasse (1900), 345-354.

[3] M. Dehn: *Ueber den Rauminhalt,* Mathematische Annalen **55** (1902), 465-478.

[4] C. F. Gauss: *"Congruenz und Symmetrie": Briefwechsel mit Gerling,* pp. 240-249 in: Werke, Band VIII, Königl. Gesellschaft der Wissenschaften zu Göttingen; B. G. Teubner, Leipzig 1900.

[5] D. Hilbert: *Mathematical Problems,* Lecture delivered at the International Congress of Mathematicians at Paris in 1900, Bulletin. Amer. Math. Soc. **8** (1902), 437-479.

[6] G. M. Ziegler: *Lectures on Polytopes,* Graduate Texts in Mathematics **152**, Springer-Verlag, New York 1995/1998.

平面上的直线构图与图的分解

第 9 章

在有关直线构图的问题中最著名的也许是Sylvester于 1893 年在一个数学问题专栏中提出的如下问题: 证明不存在不在同一条直线上的有限点集使得任意一条经过其中两点的直线都经过第三个点.

QUESTIONS FOR SOLUTION.

11851. (Professor SYLVESTER.)—Prove that it is not possible to arrange any finite number of real points so that a right line through every two of them shall pass through a third, unless they all lie in the same right line.



J. J. Sylvester

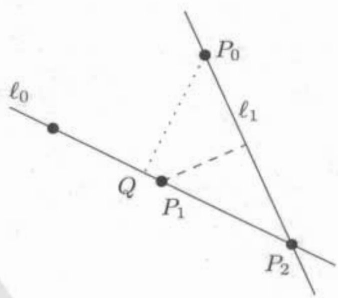
Sylvester本人当时有没有给出这个命题的证明我们无从知晓, 但 40 年后 Tibor Gallai [Grünwald] 给出了一个正确的证明. 从而, 下面的定理以 Sylvester 和 Gallai 共同命名. Gallai 之后又有几个其他的证明出现, 而属于 L.M. Kelly 的如下证明也许是其中最好的一个.

定理 1. 由平面上不共线的 n 个点所确定的直线中存在一条恰好经过其中的两个点.

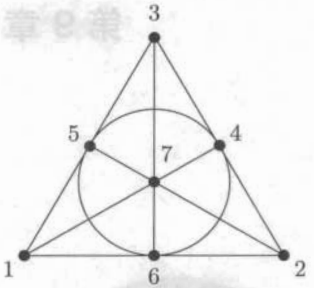
■ **证明.** 令 $\mathcal{P}$ 为给定的点集, 考虑集合 $\mathcal{L}$ 为所有经过 $\mathcal{P}$ 中至少两个点的直线. 在所有满足 P 不在 ℓ 上的 (P,ℓ) 对中, 选择一对 (P_0,ℓ_0) 使得 P_0 到 ℓ_0 的距离最短, 令 Q 为直线 ℓ_0 上距离 P_0 最近的点 (也就是说, 在 P_0 到 ℓ_0 的垂线上).

断言. ℓ_0 是满足定理的直线!

如果不是, 那么 ℓ_0 至少含有 $\mathcal{P}$ 中的三个点, 其中的两点, 设它们为 P_1 和 P_2, 落在 Q 的同侧. 我们假设 P_1 落在 Q 和 P_2 之间, 不排除 P_1 与 Q 重合的可能性. 如示意图所示, P_1 到由 P_0 和 P_2 决定的 ℓ_1 的距离比 P_0 到 ℓ_0 的距离小, 这与我们对 l_0 和 P_0 的选择矛盾! □



在这个证明中我们用到了实平面上的度量公理 (最短距离) 和顺序公理 (P_1 在 Q 和 P_2 之间). 我们是否需要这些普通点线关联公理以外的性质呢? 事实上, 一些额外的条件是需要的, 如边框所示的Fano平面: $\mathcal{P} = \{1,2,\cdots,7\}$, $\mathcal{L}$ 包含 7 条通过三点的直线, 其中包含"直线" $\{4,5,6\}$. 任何两点决定唯一的一条直线, 从而关联公理满足. 然而, 没有恰好通过两个点的直线. 从而根据Sylvester-Gallai定

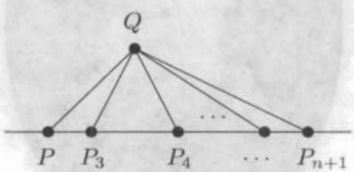


理, Fano 平面不能被镶嵌到一个实平面上, 使得这七个共线的三点组都落在实直线上: 一定会有一条是 "弯"的.

然而, Coxeter证明了在Sylvester-Gallai定理的证明中, 顺序公理就足够了. 因此, 由 Euler 公式我们可以推导出一种不需要任何度量性质的证明方法 (参见第 11 章).

Paul Erdős 和Nicolaas G. de Brujin利用Sylvester-Gallai定理得到了另一个关于实平面上点和线的著名结论. 但正如Erdős 和 de Brujin 所注意到的, 这个结论适用于更一般的任意点线系统. 过后我们将讨论更一般的结果.

定理 2. 令 P 为平面上不共线的 $n \geqslant 3$ 个点构成的集合, 则由穿过至少两个点的直线组成的集合 $\mathcal{L}$ 中至少有 n 条直线.



■ **证明.** $n=3$ 的情况很显然. 现在我们对 n 做归纳. 令 $|\mathcal{P}|=n+1$. 由上一个定理知存在一条直线 $\ell_0 \in \mathcal{L}$ 恰好经过 $\mathcal{P}$ 中的两个点, 设这两个点是 P 和 Q. 考虑集合 $\mathcal{P}'=\mathcal{P}\backslash\{Q\}$ 和由 $\mathcal{P}'$ 决定的直线集合 $\mathcal{L}'$. 如果 $\mathcal{P}'$ 的点不共线, 那么由归纳假设 $|\mathcal{L}'| \geqslant n$, 加上 $\mathcal{L}$ 中的 ℓ_0, 从而 $|\mathcal{L}| \geqslant n+1$. 如果相反, $\mathcal{P}'$ 中的点共线, 那么我们用 "铅笔" 就可画出正好 $n+1$ 条直线. □

现在, 正如所承诺的, 我们把命题推广, 这将应用到一般得多的 "关联几何".

定理 3. 假设 X 为一个有 $n \geqslant 3$ 个元素的集合, $A_1, \cdots, A_m$ 是 X 的真子集使得 X 的每对元素刚好出现在一个 A_i 中. 那么 $m \geqslant n$.

■ **证明.** 这个简洁而充满灵感的证明由 Motzkin 和 Conway 给出. 对任意 $x \in X$, 令 r_x 是包含 x 的 A_i 的个数 (由假设, $2 \leqslant r_x < m$). 现在如果 $x \notin A_i$, 那么 $r_x \geqslant |A_i|$(因为 $|A_i|$ 个包含 x 与 A_i 中的某个元素的集合必须是不同的集合). 假设 $m<n$ 那么 $m|A_i| < n r_x$, 于是 $m(n-|A_i|) > n(m-r_x)$ 对每个 $x \notin A_i$ 都成立. 所以我们得到

$$1=\sum_{x \in X} \frac{1}{n}=\sum_{x \in X} \sum_{A_i: x \notin A_i} \frac{1}{n(m-r_x)}>\sum_{A_i} \sum_{x: x \notin A_i} \frac{1}{m(n-|A_i|)}$$

$$=\sum_{A_i} \frac{1}{m}=1,$$

这不可能. □

下面是另一个非常简短的证明, 用到了线性代数. 令 B 是 $(X; A_1, \cdots, A_m)$ 的关联矩阵, 也就是说, B 的行以 X 中元素为指标, 列

以 $A_1, \cdots, A_m$ 为指标, 并且

$$B_{xA} := \begin{cases} 1 & \text{如果 } x \in A \\ 0 & \text{如果 } x \notin A. \end{cases}$$

考虑乘积 BB^T. 对 $x \neq x'$ 我们有 $(BB^T)_{xx'} = 1$, 因为 x 和 x' 恰好同时出现在一个 A_i 中, 因此

$$BB^T = \begin{pmatrix} r_{x_1}-1 & 0 & \cdots & 0 \\ 0 & r_{x_2}-1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & r_{x_n}-1 \end{pmatrix} + \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

因为第一个矩阵是正定的 (它只有正的特征值), 第二个矩阵是半正定的 (它的特征值是 n 和 0), 所以 BB^T 是正定的. 特别地, 它是可逆的, 故 $\text{rank}(BB^T) = n$. 从而 $n \times m$- 矩阵 B 的秩 $\geqslant n$, 这便可推出 $n \leqslant m$, 因为秩不会超过列数.

让我们更进一步, 转向图论. (在本章附录我们将看到一些有关图论的基本知识). 稍微思考一下我们便可发现下面的命题和定理 3 是等价的:

□

如果我们将一个完全图 K_n 分解成 m 个不同于 K_n 的团, 使得每条边恰好属于一个团, 那么 $m \geqslant n$.

事实上, 将 X 对应到 K_n 的顶点集, A_i 对应到团的顶点集, 便得到上述命题.

我们的下一个任务是将完全图 K_n 分解成一些完全二部图使得每条边都恰好属于一个完全二部图. 有一个简单的方法来做到它, 记顶点为 $\{1, 2, \cdots, n\}$. 首先将顶点 1 与其他所有顶点相连得到一个完全二部图 $K_{1,n-1}$, 我们称之为一个星图. 然后将 2 与 $3, \cdots, n$ 相连得到星图 $K_{1,n-2}$. 重复这样做, 我们将 K_n 分解成星图 $K_{1,n-1}$, $K_{1,n-2}, \cdots, K_{1,1}$. 这样的分解用到了 $n-1$ 个完全二部图. 还可以做得更好, 用更少的二部图来完成这个任务吗? 答案是否定的. 下面是 Ron Graham 和 Henry O. Pollak 得到的结论:

定理 4. *如果 K_n 被分解成完全二部图 $H_1, \cdots, H_m$, 那么 $m \geqslant n-1$.*

有趣的是, 与 Erdős-de Bruijin 定理不同, 这个定理并没有已知的组合证明! 所有的证明方法都用到了线性代数. 在所有大同小异的想法中让我们看看 Tverberg 的这个, 它也许是最清楚的.



将 K_5 分解成 4 个完全二部子图

■ **证明.** 令完全图 K_n 的顶点为 $\{1,\cdots,n\}$, 令 L_j, R_j 是对应于完全二部图 H_j $j=1,\cdots,m$ 的顶点集. 对每个顶点 i 我们引入一个变量 x_i. 既然 $H_1,\cdots,H_m$ 组成了 K_n, 我们有

$$\sum_{i<j} x_i x_j \;=\; \sum_{k=1}^{m}\left(\sum_{a\in L_k} x_a\cdot\sum_{b\in R_k} x_b\right). \qquad (1)$$

现在假定这个命题是错的, 即 $m<n-1$. 那么线性方程组

$$\begin{aligned} x_1+\cdots+x_n &= 0,\\ \sum_{a\in L_k} x_a &= 0 \qquad (k=1,\cdots,m)\end{aligned}$$

的方程个数比变量个数少, 从而存在非平凡解 $c_1,\cdots,c_n$. 由 (1) 我们得到

$$\sum_{i<j} c_i c_j \;=\; 0.$$

但这又推出

$$0 \;=\; (c_1+\cdots+c_n)^2 \;=\; \sum_{i=1}^{n} c_i^2 + 2\sum_{i<j} c_i c_j \;=\; \sum_{i=1}^{n} c_i^2 \;>\; 0,$$

矛盾! 证明完成. □

附录: 基本的图论概念



一个有 7 个顶点和 11 条边的图 G. 它有一个自环, 一条二重边和一条三重边.

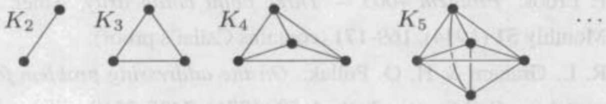
图是最基本的数学结构之一. 它有许多不同的表达方法. 抽象地, 图可以表示为 $G=(V,E)$, 其中 V 是顶点的集合, E 是边的集合, 每条边 $e\in E$ "连接" 了两个顶点 $v,w\in V$. 我们只考虑有限图, 也就是 V 和 E 都是有限的.

通常, 我们只考虑简单图: 也就是说我们不允许图中存在自环 (两个端点重合的边), 也不存在多重边 (有同一对端点的多条边). 图的两个顶点称为是邻接或相邻的, 如果它们是一条边的两个端点. 一个顶点和一条边被称为是关联的, 如果该顶点是这条边的一个端点.

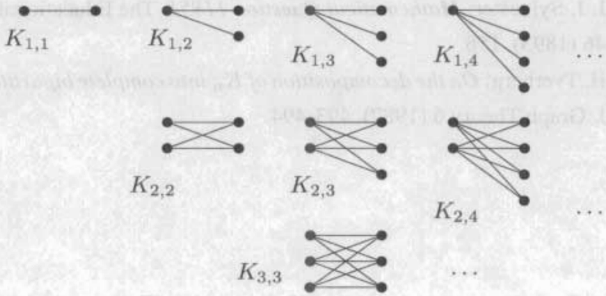
两个图 $G=(V,E)$ 和 $G'=(V',E')$ 称为是同构的, 如果存在保持边和顶点关系不变的双射 $V\to V'$ 和 $E\to E'$ (一个悬而未决的问题是如何有效地判断两个图是不是同构的).

我们称 $G' = (V', E')$ 为 $G = (V, E)$ 的一个子图, 如果 $V' \subseteq V$, $E' \subseteq E$, 并且每条边 $e' \in E'$ 在 G' 中与在 G 中有相同的端点. 进一步, 我们称 G' 为 G 的一个诱导子图, 如果所有 G 中连接 G' 的顶点的边也是 G' 中的边.

下面是一些重要的 (简单) 图:



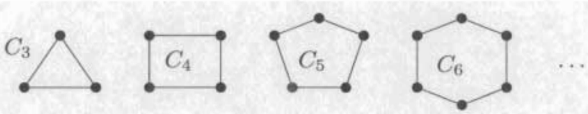
有 n 个顶点和 $\binom{n}{2}$ 条边的完全图 K_n



有 $m+n$ 个顶点和 mn 条边的完全二部图 $K_{m,n}$



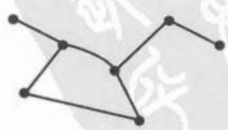
具有 n 个顶点的路 P_n



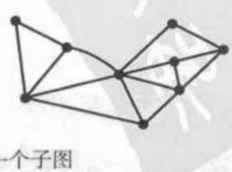
具有 n 个顶点的圈 C_n

许多关于图的概念是直观的: 例如, 图 G 称作是连通的, 如果 G 中任意两个不同的顶点间有路或称路径相连, 或者等价地说, G 不能被分解成两个非空的顶点集不交的子图.

我们再引入一些术语作为图论基本概念论述的结束: G 的一个团表示 G 的一个完全子图. G 的一个独立集表示一个 G 的没有边的诱导子图, 也就是说, G 中一个相互之间没有连边的顶点子集. 一个图称为是森林, 如果该图中没有圈. 一棵树表示一个连通的森林. 最后, 图 $G = (V, E)$ 称为是二部图, 如果它和一个完全二部图的子图同构, 也就是说, 它的顶点集可以写成两个独立集的并 $V = V_1 \cup V_2$.



是



的一个子图

参考文献

[1] N. G. de Bruijn & P. Erdős: *On a combinatorial problem,* Proc. Kon. Ned. Akad. Wetensch. **51** (1948), 1277-1279.

[2] H. S. M. Coxeter: *A problem of collinear points,* Amer. Math. Monthly **55** (1948), 26-28 (contains Keuy's proof).

[3] P. Erdős: *Problem 4065 — Three point collinearity,* Amer. Math. Monthly **51** (1944), 169-171 (contains Callai's proof).

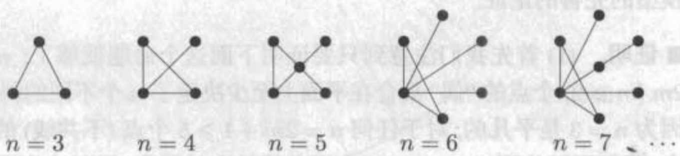
[4] R. L. Graham & H. O. Pollak: *On the addressing problem for loop switching,* Bell System Tech. J. **50** (1971), 2495-2519.

[5] J. J. Sylvester: *Mathematical Question 11851,* The Educational Times **46** (1893), 156.

[6] H. Tverberg: *On the decomposition of K_n into complete bipartite graphs,* J. Graph Theory **6** (1982), 493-494.

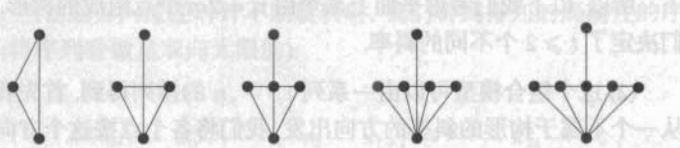
斜率问题

在往下看之前，请你自己尝试在平面上画出一定个数的点，使得这些点连出的斜率"较少"。当然，我们假定在 $n \geqslant 3$ 时这些点不共线. 回顾第 9 章 Erdős 和 de Bruijn 关于"平面上直线"的定理：n 个点至少确定 n 条不同的直线. 当然，这些直线很多可能是平行的，从而决定了同一个斜率.



$n=3$ 3 个斜率 $n=4$ 4 个斜率 $n=5$ 4 个斜率 $n=6$ 6 个斜率 $n=7$ 6 个斜率 $\cdots$

或



$n=3$ 3 个斜率 $n=4$ 4 个斜率 $n=5$ 4 个斜率 $n=6$ 6 个斜率 $n=7$ 6 个斜率 $\cdots$

n 较小时的几个情况

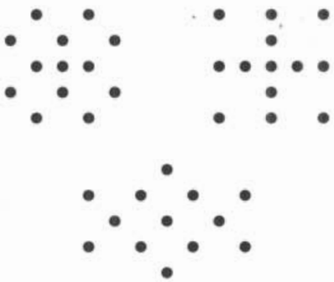
在尝试了几个较小的 n 后，也许你会猜出 Scott 在 1970 年得到的定理：

> **定理.** 平面上 $n \geqslant 3$ 个不共线的点至少可确定 $n-1$ 个不同的斜率，其中等号仅当 n 为大于等于 5 的奇数时可能成立.

上面画出的例子是两个无穷序列的前几个构形，它们表明定理所给出的是最佳的情况：$n \geqslant 5$ 且为奇数时，存在平面上的 n 个点恰

好决定了 $n-1$ 个不同的斜率, 而对于其他的 $n\,(n \geqslant 3)$ 存在平面上的 n 个点恰好决定了 n 个不同的斜率.

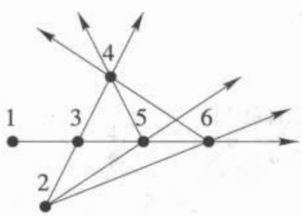
然而, 我们上面所画的构形远不是唯一的. 例如, Jamison 和 Hill 描述了 4 族平面图, 每一族有无穷多个, 且其中的 n 个点 (n 是奇数) 恰好决定了 $n-1$ 个不同的斜率 ("极端斜率构形 (slope-critical configurations)"). 另外, 他们列举了 102 个不属于某个无穷族的 "零散" 的例子, 这些例子大多由大规模的计算机搜索得到.



由 Jamison-Hill 给出的三个漂亮的零散例子

传统的经验告诉我们如果极限情况的构形是多种多样的无规律的, 那么这个极值问题获得准确解答将非常困难. 确实, 关于极端斜率构形的结构有许多研究 (见 [2]), 但是却没有这种构形的分类. 然而, 上面的定理有一个简单的证明方法, 这个方法包含了两个要素: 将问题简化为一个由 Eli Goodman 和 Ricky Pollack 给出的有效的组合模型, 以及一个 Peter Ungar 在 1982 年给出的有关这个组合模型的完善的论证.

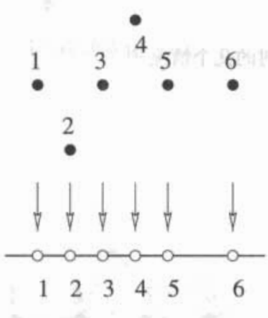
■ **证明.** **(1)** 首先我们注意到只要证明下面这个命题就够了: $n = 2m\,(m \geqslant 2)$ 个点的 "偶" 集合在平面上至少决定了 n 个不同的斜率. 因为 $n=3$ 是平凡的, 对于任何 $n = 2m+1 \geqslant 5$ 个点 (不共线) 的集合, 我们可以找到 $n-1 = 2m$ 个不共线的点的子集, 已经决定了至少 $n-1$ 个不同的斜率.



6 个点确定了 6 个不同斜率的构形

所以, 以下我们考虑平面上某个由 $n=2m$ 个点组成的构形. 它们决定了 $t \geqslant 2$ 个不同的斜率.

(2) 这个组合模型可以由一系列 $1, \cdots, n$ 的排列得到. 首先我们从一个不属于构形的斜率的方向出发, 我们将各个点按这个方向的投影排列的顺序标记为 $1, \cdots, n$. 所以, $\pi_0 = 123\cdots n$ 代表在起始方向各点的顺序.



这里, 垂直方向导出的排列 $\pi_0 = 123456$.

然后将初始方向按逆时针方向旋转, 同时观察投影及其排列的变化. 排列发生变化当且仅当旋转经过该构形的一个斜率方向时.

但排列的变化并不是随机和任意的: 当方向经过了 180° 的旋转后, 我们得到了一排列的序列:

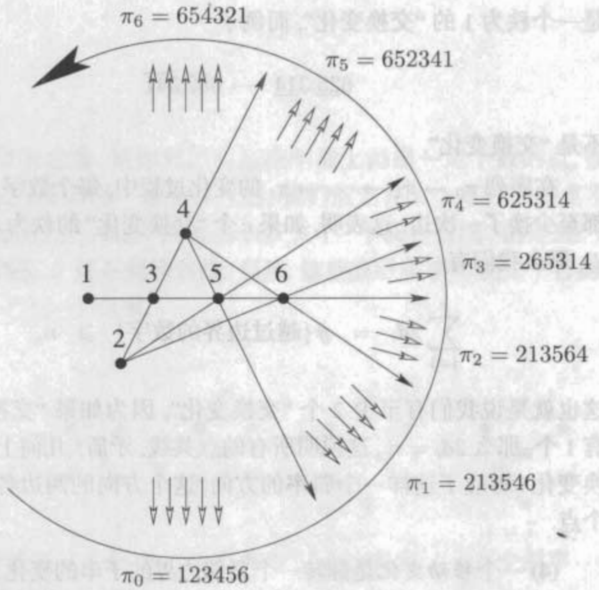
$$\pi_0 \to \pi_1 \to \pi_2 \to \cdots \to \pi_{t-1} \to \pi_t$$

这一排列的序列有如下特殊性质:

- 序列从 $\pi_0 = 123...n$ 开始, 以 $\pi_t = n...321$ 结束.
- 排列的个数 t 正是构形中不同斜率的个数.
- 在这些排列中, 每对 $i < j$ 恰好被交换一次次序. 这说明, 从 $\pi_0 =$

123...n 到 $\pi_t = n...321$ 的过程中, 只有递增的子串被翻转了.

- 每次排列的改变包含了一个或多个不交的递增子串的翻转 (对应于改变发生处斜率相同的一条或多条直线)



由例子所产生的一个排列序列

当初始方向按逆时针不断旋转时, 我们看到排列的周期性的序列 (将序列看做是双向无限的):

$$\cdots \to \pi_{-1} \to \pi_0 \to \cdots \to \pi_t \to \pi_{t+1} \to \cdots \to \pi_{2t} \to \cdots,$$

其中对任意 $i\pi_{i+t}$ 是 π_i 的翻转, 从而对任意 $i \in \mathbb{Z}\pi_{i+2t} = \pi_i$.

我们将证明每个满足上述条件的序列 (其中 $t \geqslant 2$) 的长度都满足 $t \geqslant n$.

(3) 证明的关键是将每一个排列分割成长为 $m = \frac{n}{2}$ 的 "左半边" 和 "右半边", 并计算跨过边界的数字个数.

我们称 $\pi_i \to \pi_{i+1}$ 是一个交换变化, 如果这个变化包含一个跨 "边界" 的子串的翻转. 我们称这个 "交换变化" 的秩是 d, 如果它把 $2d$ 个数字换过边界, 此时被翻转的子串恰有 d 个数字在一边, 至少 d 个数字在另一边. 从而例子



一个 "交换变化"

$$\pi_2 = 2\underline{13{:}564} \longrightarrow \overline{265{:}314} = \pi_3$$

是一个秩为 2 的“交换变化”(它把 1,3,5,6 交换过由“:”表示的边界),

$$65\underline{2{:}341} \longrightarrow 65\overline{4{:}321}$$

是一个秩为 1 的“交换变化”,而例子

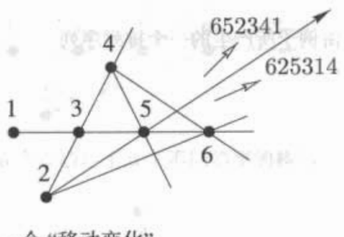
$$6\underline{25}{:}3\underline{14} \longrightarrow 6\overline{52}{:}3\overline{41}$$

不是“交换变化”.

在序列 $\pi_0 \to \pi_1 \to \cdots \to \pi_t$ 的变化过程中,每个数字 $1, 2, \cdots, n$ 都至少换了一次边. 这表明,如果 c 个“交换变化”的秩为 $d_1, d_2, \cdots, d_c$,那么我们有

$$\sum_{i=1}^{c} 2d_i \ = \ \#\{\text{越过边界的数字}\} \ \geqslant \ n.$$

这也就是说我们有至少 2 个“交换变化”,因为如果“交换变化”只有 1 个,那么 $2d_i = n$,这说明所有的点共线,矛盾!几何上,一个“交换变化”对应了这样一个斜率的方向,这个方向的两边各有少于 m 个点.



一个“移动变化”

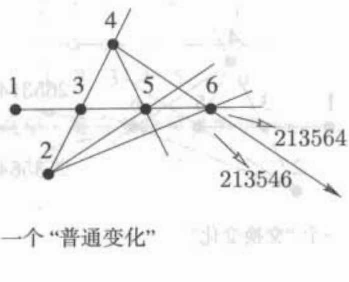
(4) 一个*移动变化*是翻转一个紧邻边界的子串的变化,但不越过边界. 例如,

$$\pi_4 \ = \ 6\underline{25}{:}3\underline{14} \longrightarrow 6\overline{52}{:}3\overline{41} \ = \ \pi_5$$

是一个“移动变化”. 几何上,一个“移动变化”对应了这样一条直线斜率的方向,这个方向的一边恰有 m 个点,从而另一边最多有 $m-2$ 个点.

既不是“交换变化”又不是“移动变化”的变化称为*普通变化*. 下面便是一个“普通变化”的例子:

$$\pi_1 \ = \ 213{:}5\underline{46} \longrightarrow 213{:}5\overline{64} \ = \ \pi_2.$$



一个“普通变化”

这样每个变化是交换的、移动的、普通的三者之一. 我们用 T, C, O 代表这三种类型:“交换变化”,“移动变化”和“普通变化”. 记秩为 d 的“交换变化”为 $C(d)$. 针对我们的小小例子有

$$\pi_0 \xrightarrow{T} \pi_1 \xrightarrow{O} \pi_2 \xrightarrow{C(2)} \pi_3 \xrightarrow{O} \pi_4 \xrightarrow{T} \pi_5 \xrightarrow{C(1)} \pi_6,$$

或者更简单地将这个序列记作 $T, O, C(2), O, T, C(1)$.

(5) 为完成证明,我们需要如下两个事实:

在任意两个"交换变化"之间, 至少有一个"移动变化".

在任意一个秩为 d 的"交换变化"和其后的一个"移动变化"之间, 至少有 $d-1$ 个"普通变化".

事实上, 在一次秩为 d 的"交换变化"后, 边界包含在一个长为 $2d$ 的对称递减的子串之中, 边界两边各有 d 个数字. 下一个"交换变化"必须伴随一个长至少为 2 的跨边界的递增子串. 但是只有"移动变化"能改变边界是否在一个递增的子串中, 从而第一个事实得证. 对于第二个事实, 注意到每一个"普通变化" (翻转某递增子串) 只能把递减的 $2d$ - 子串在边界的每一侧缩短一个数字. 同时, 只要递减子串有至少个 4 数字, "移动变化"就是不可能的. 这证明了第二个事实.

如果我们构造这个排列序列时使用相同的初始投影但用顺时针而不是逆时针旋转, 那么我们将得到一个翻转的排列序列. 从而这个序列必然满足第二个事实的相反的情况:

在一个"移动变化"到下一个秩为 d 的"交换变化"之间有至少 $d-1$ 个"普通变化".

(6) 在 (2) 中得到的无穷长的 T-O-C- 模式排列序列是长为 t 的序列 $\pi_0 \longrightarrow \cdots \longrightarrow \pi_t$ 的一再重复. 从而结合 (5) 中的事实, 我们看到在变化的无穷长的序列中秩为 d 的"交换变化"必然嵌入到 T-O-C- 模式的下列序列中

$$T, \underbrace{O, O, \cdots, O}_{\geqslant d-1}, C(d), \underbrace{O, O, \cdots, O}_{\geqslant d-1}, \qquad (*)$$

这个序列的长度至少为 $1+(d-1)+1+(d-1)=2d$.

考虑无限序列的一个长度为 t 的有限片断, 我们可以假设它由一个"移动变化"开始. 这个片段包含 $(*)$ 中类型的子串, 也许再加上其他的 T. 这表明其长度 t 满足

$$t \geqslant \sum_{i=1}^{c} 2d_i \geqslant n,$$

这便完成了证明. □

参考文献

[1] J. E. Goodman & R. Pollack: *A combinatorial perspective on some problems in geometry,* Congressus Numerantium **32** (1981), 383-394.

[2] R. E. Jamison & D. Hill: *A catalogue of slope-critical configurations,* Congressus Numerantium **40** (1983), 101-125.

[3] P. R. Scott: *On the sets of directions determined by n points,* Amer. Math. Monthly **77** (1970), 502-505.

[4] P. Ungar: *$2N$ noncollinear points determine at least $2N$ directions,* J. Combinatorial Theory, Ser. A **33** (1982), 343-347.

Euler 公式的三个应用

第 11 章



Leonhard Euler

如果一个图可以被画在平面 $\mathbb{R}^2$ (或者等价地, 二维球面 S^2) 上面没有交叉边, 那么称这个图是*平面的*. 如果这样的一种画法已经给出并且固定了, 那么称这个图为*平面图*. 任意这种画法都把平面或者球面分割成有限个连通区域, 包括外面 (无边界) 的区域, 我们把这些区域叫做*面*. Euler 公式对平面图的顶点数、边数、面数之间建立了一个优美的关系. Euler 在 1750 年给他的朋友 Goldbach 的信中第一次提到了这个公式, 但当时他并没有给出完整的证明. 在 Euler 公式的多种证明中, 我们给出 von Staudt 在 1847 年《Geometrie der Lage》一书中做出的证明. 这是一个优美的、"自对偶" 的且不需要归纳法的证明.

Euler 公式. *如果 G 是一个有 n 个顶点, e 条边和 f 个面的连通平面图, 那么*

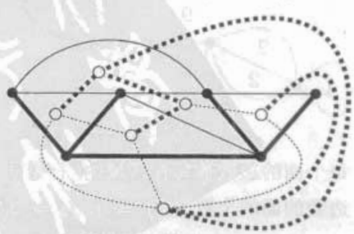
$$n - e + f = 2.$$

■ **证明.** 令 $T \subseteq E$ 是 G 的一个生成树的边集, 生成树是指最小的连接 G 的每个顶点的子图. 由最小性假设可以推出, 生成树不含圈.



一个平面图 G: $n = 6, e = 10, f = 6$

我们现在需要引入对偶图的概念: 为了构造 G 的*对偶图* G^*, 我们在 G 的每个面的内部画一个顶点, 对应 G 的面的公共边界对 G^* 中的这些点连线. 如果两个面有几条共同边界, 就在这两个面中的点间连接几条不同的边. (从而即使原图 G 是简单图, G^* 也有可能有多重边.)

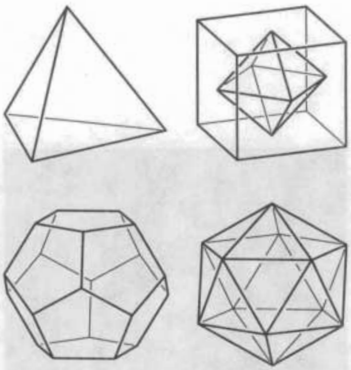


G 和 G^* 中的对偶生成树

考虑对应 G 中边集 $E \backslash T$ 的对偶图中的边集 $T^* \subseteq E^*$. 因为 T 不含圈, T^* 中的边连接了所有的面; 但 T^* 也不含圈, 否则它将把 G 的圈中的点与圈外的点分离 (这是不可能的, 因为 T 是生成子图, 并且 T 和 T^* 的边不交). 从而 T^* 是 G^* 的一个生成树.

对于每个树, 顶点个数比边数大 1. 为看清这点, 我们选择一个顶点作为根, 并把所有边指定为从根离开的方向: 通过将每条边对

应它指向的顶点, 构成了一个除了根之外的所有顶点到边的双射. 把它分别应用到树 T 和 T^* 上, 我们得到 $n = e_T + 1$ 和 $f = e_{T^*} + 1$. 将两个等式相加我们得到 $n + f = (e_T + 1) + (e_{T^*} + 1) = e + 2$. □

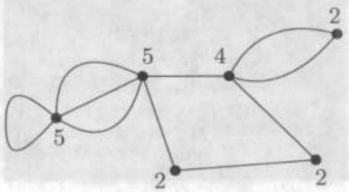


五个 Plato 立体

这样, Euler 公式给出了一个几何拓扑中很强的数值结论: 无论一有限图是可以 被画在一个平面上还是一个球面上, 其点数、线数和面数总满足 $n - e + f = 2$.

许多熟知的和经典的结论可以由 Euler 公式推出. 其中有正规凸多面体 (Plato 立体) 的分类, K_5 和 $K_{3,3}$ 不是可平面化的 (参见下面所证) , 还有著名的五色定理 (每个平面地图可以被不超过 5 种颜色着色, 使得相邻国家的颜色不同) . 但对于五色定理, 我们有不用 Euler 公式的更好的证明, 见第 30 章.

这一章收集了以 Euler 公式为核心的三个定理的漂亮证明. 前两个对 Sylvester-Gallai 定理和对两色点构形定理的证明将 Euler 公式巧妙地与另外的基本图中参数之间的数量关系结合. 让我们先来看看这些参数.



每个顶点的度数已在图中标出, 对应于各个度数的顶点个数为 $n_2 = 3$, $n_3 = 0, n_4 = 1, n_5 = 2$.

以一个顶点为端点的边的个数称为这个顶点的**度数** (其中每个自环算两次). 令 n_i 表示图 G 中度数是 i 的顶点个数. 根据顶点的度数来计数顶点个数, 我们有

$$n = n_0 + n_1 + n_2 + n_3 + \cdots \tag{1}$$

另一方面, 每条边有两个端点, 它对所有度数的和贡献 2, 从而我们有

$$2e = n_1 + 2n_2 + 3n_3 + 4n_4 + \cdots \tag{2}$$

你可以把这个等式理解为用两种方法同时计算边的端点数, 也就是所有的边 — 顶点关联关系. 顶点的**平均度数** $\bar{d}$ 为

$$\bar{d} = \frac{2e}{n}.$$



每个面的边数被写在区域内, 有相同边数的面的个数为 $f_1 = 1$, $f_2 = 3$, $f_4 = 1$, $f_9 = 1$, 以及对其他指标 $f_i = 0$.

下面我们通过面的边数来计数一个平面图的面数: 一个*k*- 面指一个有 k 条边的面 (如果一条边的两面都是这个面的边界, 那么这条边要被计算两次!). 令 f_k 是 k- 面的个数. 计算面的个数我们有

$$f = f_1 + f_2 + f_3 + f_4 + \cdots \tag{3}$$

通过作为面的边界来计算边数, 我们有

$$2e = f_1 + 2f_2 + 3f_3 + 4f_4 + \cdots \tag{4}$$

像从前一样，我们可以把这些理解为用两种方法同时计算所有的边 — 面关联关系. 注意到面的平均边数为

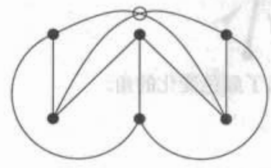
$$\overline{f} = \frac{2e}{f}.$$

下面我们通过它们，再结合 Euler 公式，很快便可推出完全图 K_5 和完全二部图 $K_{3,3}$ 不是平面图. 对 K_5 的一个假想的平面画法，我们有 $n=5, e=\binom{5}{2}=10$, 从而 $f=e+2-n=7$ 并且 $\overline{f}=\frac{2e}{f}=\frac{20}{7}<3$. 但如果面的平均边数小于 3, 那么这个嵌入中必然有一个面只有至多 2 条边界，这是不可能的.



K_5 在平面上有一个交叉处的画法

相似地，对于 $K_{3,3}$ 我们有 $n=6, e=9$, 并且 $f=e+2-n=5$, 从而 $\overline{f}=\frac{2e}{f}=\frac{18}{5}<4$, 而 $K_{3,3}$ 是简单图并且是二部的，它的每个圈长至少为 4 , 从而不可能.



$K_{3,3}$ 在平面上有一个交叉处的画法

关于 f_i 的等式 (3), (4) 看上去和关于 n_i 的等式 (1), (2) 相似，这并不是偶然的. 它们可以通过我们前面解释的对偶图构造 $G \to G^*$ 互相转化.

由双计数恒等式，我们得到 Euler 公式的如下重要的 “局部” 推论.

命题. 令 G 是顶点数 $n>2$ 的简单平面图，那么

(A) G 有一个度数最多是 5 的顶点.

(B) G 最多有 $3n-6$ 条边.

(C) 如果 G 的边被两种颜色着色，那么它有一个顶点围绕该点的边沿着圆环的次序最多经历了两次颜色的变化.

■ **证明.** 对于这 3 条中的每一条，我们都可以假设 G 是连通的.

(A) 每一面至少有 3 条边 (由于 G 是简单的), 因此由 (3) 和 (4) 得

$$\begin{aligned} f &= f_3 + f_4 + f_5 + \cdots, \\ 2e &= 3f_3 + 4f_4 + 5f_5 + \cdots, \end{aligned}$$

因此 $2e-3f \geqslant 0$.

现在如果每个顶点的度数至少为 6, 那么由 (1) 和 (2) 我们得到

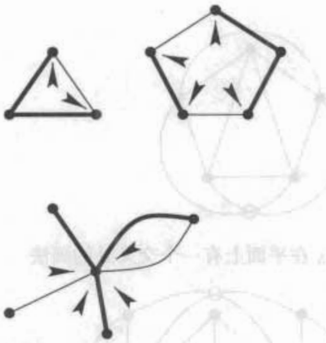
$$\begin{aligned} n &= n_6 + n_7 + n_8 + \cdots, \\ 2e &= 6n_6 + 7n_7 + 8n_8 + \cdots, \end{aligned}$$

因此 $2e-6n \geqslant 0$,

结合这两个不等式, 我们得到

$$6(e-n-f) = (2e-6n)+2(2e-3f) \geqslant 0,$$

因此 $e \geqslant n+f$, 与 Euler 公式矛盾.



箭头指出了颜色变化的角.

(B) 在 (A) 的第一步, 我们已得到 $2e-3f \geqslant 0$, 因此由 Euler 公式得

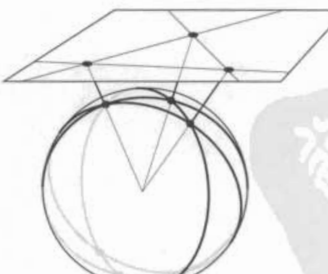
$$3n-6 = 3e-3f \geqslant e.$$

(C) 令 c 为颜色发生变化的角的数目. 假设命题不成立, 由于在每一个顶点处变化次数均为偶数, 我们得到 $c \geqslant 4n$ 个颜色变化的角. 现在每个有 $2k$ 或 $2k+1$ 条边的面有最多 $2k$ 个这样的角, 因此我们可以得出

$$\begin{aligned}
4n \leqslant c &\leqslant 2f_3+4f_4+4f_5+6f_6+6f_7+8f_8+\cdots \\
&\leqslant 2f_3+4f_4+6f_5+8f_6+10f_7+\cdots \\
&= 2(3f_3+4f_4+5f_5+6f_6+7f_7+\cdots) \\
&\quad -4(f_3+f_4+f_5+f_6+f_7+\cdots) \\
&= 4e-4f,
\end{aligned}$$

其中我们再次应用到了 (3) 和 (4). 从而可以得到 $e \geqslant n+f$, 又与 Euler 公式矛盾. □

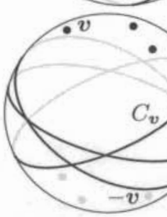
1. 再探 Sylvester-Gallai 定理



Norman Steenrod 首先发现性质 (A) 可以给出 Sylvester-Gallai 定理 (见第 9 章) 一个非常简单的证明.

Sylvester-Gallai 定理. 给定任意 $n \geqslant 3$ 个平面上的不共线的点, 一定存在一条直线经过其中恰好两个点.

■ **证明.** (由 Euler 公式推出 Sylvester-Gallai 的证明)



如果我们如图所示把 $\mathbb{R}^2$ 平面镶嵌到 $\mathbb{R}^3$ 中单位球面 S^2 上, 那么 $\mathbb{R}^2$ 中的每个点对应了球面 S^2 上的一对对径点, $\mathbb{R}^2$ 中的每条直线对应了 S^2 中的一个大圆. 从而 Sylvester-Gallai 定理等价于如下命题:

给定任何 $n \geqslant 3$ 对球面 S^2 上的不共圆的对径点, 总存在一个大圆恰好经过两对对径点.

对偶地, 我们把每对对径点用对应的球面上的大圆代替. 也就是说, 我们不考虑 $\pm v \in S^2$ 而是用由 $C_v := \{x \in S^2 : \langle x, v\rangle = 0\}$ 给定的正交圆去代替它. (如果 v 是球面上的北极点, 则这个 C_v 是赤道.)

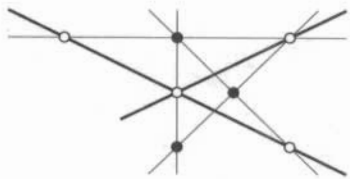
那么 Sylvester-Gallai 问题要求我们去证明:

在球面 S^2 上给定 $n \geqslant 3$ 个不共点大圆, 那么一定存在一个点恰好在两个大圆上.

但是 S^2 上的这些大圆的安排给出了一个简单平面图, 顶点是其中两个大圆的交点, 它们又把大圆分开为边. 根据构造, 所有顶点的度数都是偶数, 并且至少是 4. 从而结合性质 (A) 得出了 4 度顶点的存在性. 得证! □

2. 单色线

接下来的 Sylvester-Gallai 定理关于 "着色" 的变异形式的证明是由 Don Chakerian 给出的.



定理. *平面上任意给定有限个 "黑色" 的和 "白色" 的非共线点, 总是存在一条 "单色" 线: 即经过至少两个同色的点, 而不经过另一颜色的点的线.*

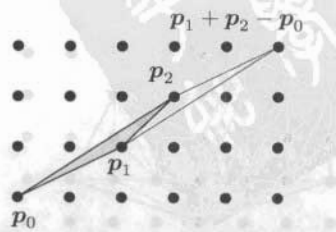
■ **证明.** 正如对于 Sylvester-Gallai 问题, 我们将问题转换成在单位球面的情形并且对偶化. 所以我们只需证明:

给定单位球面上任意有限个 "黑色" 的和 "白色" 的不共点的大圆, 总是存在一个交点, 它或者只落在白色的大圆上, 或者只落在黑色的大圆上.

而这个命题可以由性质 (C) 推出, 因为在每个顶点不同颜色大圆的交点处, 我们总是有至少 4 个颜色变化的角. □

3. Pick 定理

于 1899 年发现的 Pick 定理是一个优美而令人惊异的结论, 但同时也是 Euler 定理的一个"经典"的推论. 下面我们称一个凸多边形 $P \subseteq \mathbb{R}^2$ 是基本的, 如果它的顶点坐标都是整数 (也就是说, 它可以镶嵌到 $\mathbb{Z}^2$ 格中), 但是它不含有其他格点.



引理. *每个基本的三角形 $\Delta = \operatorname{conv}\{p_0, p_1, p_2\} \subseteq \mathbb{R}^2$ 的面积是 $A(\Delta) = \frac{1}{2}$.*

■ **证明.** 以 $p_0, p_1, p_2, p_1 + p_2 - p_0$ 为顶点的平行四边形和 $\mathbb{Z}^2$ 格对

格的基

一个 $\mathbb{Z}^2$ 格的基是一对线性无关的向量 $\boldsymbol{e}_1, \boldsymbol{e}_2$ 满足

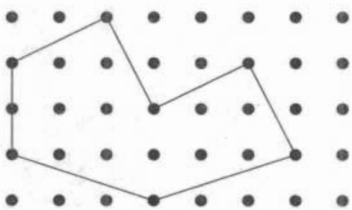
$$\mathbb{Z}^2 = \{\lambda_1 \boldsymbol{e}_1 + \lambda_2 \boldsymbol{e}_2 : \lambda_1, \lambda_2 \in \mathbb{Z}\}.$$

令 $\boldsymbol{e}_1 = \binom{a}{b}$, $\boldsymbol{e}_2 = \binom{c}{d}$, 那么由 $\boldsymbol{e}_1$, $\boldsymbol{e}_2$ 张成的平行四边形的面积是 $A(\boldsymbol{e}_1, \boldsymbol{e}_2) = |\det(\boldsymbol{e}_1, \boldsymbol{e}_2)| = |\det\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)|$. 如果 $\boldsymbol{f}_1 = \binom{r}{s}$ 和 $\boldsymbol{f}_2 = \binom{t}{u}$ 是另一组基, 那么存在一个可逆的 $\mathbb{Z}$ 矩阵 Q 使得 $\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)Q$. 既然 $QQ^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, 并且行列式的值是整数, 这可推出 $|\det Q| = 1$, 从而 $|\det(\boldsymbol{f}_1, \boldsymbol{f}_2)| = |\det(\boldsymbol{e}_1, \boldsymbol{e}_2)|$. 又因为 $A(\binom{1}{0}, \binom{0}{1}) = 1$, 所以所有基张成的平行四边形有相同的面积 1.

于下面的映射都是对称的:

$$\sigma : \boldsymbol{x} \longmapsto \boldsymbol{p}_1 + \boldsymbol{p}_2 - \boldsymbol{x},$$

这个映射是对 $\boldsymbol{p}_1$ 到 $\boldsymbol{p}_2$ 连线的中点的反射. 从而平行四边形 $P = \Delta \cup \sigma(\Delta)$ 也是基本的, 并且它的整点平移铺满了整个平面. 从而 $\{\boldsymbol{p}_1 - \boldsymbol{p}_0, \boldsymbol{p}_2 - \boldsymbol{p}_0\}$ 是 $\mathbb{Z}^2$ 格的一个基, 它的行列式的值是 ± 1, P 的面积是 1, 从而 Δ 的面积是 $\frac{1}{2}$. (关于这些名词的解释请参见上面的方框.) □



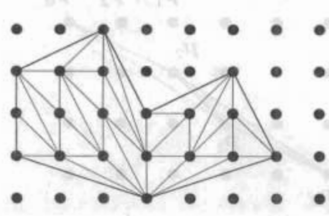
$n_{int} = 11$, $n_{bd} = 8$, 所以 $A = 14$

定理. *顶点的坐标都是整数的 (不一定凸) 多边形 $Q \subseteq \mathbb{R}^2$ 的面积是*

$$A(Q) = n_{int} + \frac{1}{2} n_{bd} - 1,$$

其中 n_{int} 和 n_{bd} 分别是 Q 内部和边界上的整点个数.

■ **证明.** 每一个这样的多边形可以由 Q 内部的 n_{int} 个格点和边界上的 n_{bd} 个格点分成小三角形, 如边栏图. (这并不是很显然, 特别是如果 Q 不要求是凸的, 但第 31 章中会给出证明.)



现在我们把这个三角剖分看成是一个平面图, 它把平面分割成一个无界的面和 $f - 1$ 个面积是 $\frac{1}{2}$ 的三角形, 从而

$$A(Q) = \frac{1}{2}(f - 1).$$

每一个三角形有 3 条边, 而 e_{int} 条内部边的每一条是两个三角形的

边界，e_{bd} 条边界中的每一条出现在一个三角形中. 从而 $3(f-1)=2e_{int}+e_{bd}$ 并且 $f=2(e-f)-e_{bd}+3$. 另外，边界上的边数和顶点数是一样的，$e_{bd}=n_{bd}$. 这两个事实结合 Euler 公式得出

$$\begin{aligned} f &= 2(e-f)-e_{bd}+3 \\ &= 2(n-2)-n_{bd}+3 \;=\; 2n_{int}+n_{bd}-1, \end{aligned}$$

从而

$$A(Q) \;=\; \tfrac{1}{2}(f-1) \;=\; n_{int}+\tfrac{1}{2}n_{bd}-1. \qquad \Box$$

参考文献

[1] G. D. Chakerian: *Sylvester's problem on collinear points and a relative,* Amer. Math. Monthly **77** (1970), 164-167.

[2] G. Pick: *Geometrisches zur Zahlenlehre,* Sitzungsberichte Lotos (Prag), Natur-med. Verein für Böhmen **19** (1899), 311-319.

[3] K. G. C. von Staudt: *Geometrie der Lage,* Verlag der Fr. Korn'schen Buchhandlung, Nürnberg 1847.

[4] N. E. Steenrod: *Solution 4065/Editorial Note,* Amer. Math. Monthly **51** (1944), 170-171.

Cauchy 的刚性定理

第 12 章

关于三维多面体的 Cauchy 刚性定理是一个依赖于 Euler 公式 (特别是前一章中命题的 (C) 部分) 的著名结果.

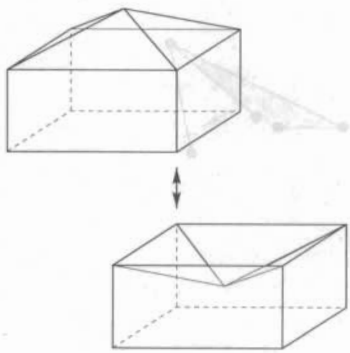
接下来涉及的多胞体和多面体的全等和组合等价都已经在第 8 章 Hilbert 第三问题的附录中作过介绍.

定理. *如果两个三维凸多面体 P 和 P' 是组合等价的, 并且各个对应面是全等的, 那么对应的相邻面的夹角也是相等的 (也就是说 P 和 P' 是全等的).*



Augustin Cauchy

如旁边的图中所示的两个三维多面体, 它们是组合等价的, 并且各个对应面是全等的. 但这两个多面体并不全等, 并且其中只有一个是凸的. 从而凸多面体这个假设对 Cauchy 定理是必需的.

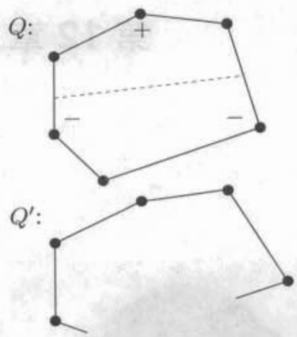


■ **证明.** 下面的证明基本上是 Cauchy 给出的原证明. 假设给定两个有全等面的凸多面体 P 和 P'. 我们着色 P 的边如下: 如果边对应的二面角在 P' 中比 P 中的大就把这条边着成黑色 (或称 "正的"), 如果 P' 的比 P 的小, 就着成白色或称 "负的".

P 的黑边和白边在 P 的表面形成一个二色的平面图, 通过一源点在 P 的内部的径向投射, 我们把这个平面图镶嵌到单位球面上去. 如果 P 和 P' 有对应的不等的二面角, 那么这个图不是空图. 由上一章性质 (C) 我们知道有一个顶点 p 与至少一条黑边或白边相邻, 使得绕这个顶点的边颜色最多变化两次 (沿圆环的次序).

现在我们以 p 点为中心以 ε 为半径作一个小球 S_ε, 与 P 相交, 我们以 p 的对应点 p' 为中心也作一个同样半径的球 S'_ε, 与 P' 相交. 由于 P 和 P' 的各个面全等, 并且我们选择了相同的半径 ε, 在 S_ε 与 S'_ε 上我们得到凸球面多边形 Q 和 Q' 使得相应的弧也有相同的长度.

现在我们对 Q 的比它在 Q' 中对应的角小的角标记 $+$, 比它在 Q' 中对应的角大的角标记 $-$. 也就是说, 当把 Q 移动到 Q', 标

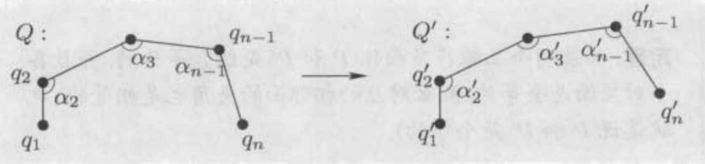


记 + 的角是“打开的”，标记 − 的角是“关闭的”，而所有的边长和没有标记的角是相等的.

从对 p 的选择我们知道以 p 为顶点的角总要出现记号 + 或者 −，并且沿圆环的次序最多有两次 +/− 变换. 如果只有 + 或者 −，那么下面的引理会推出 P 和 P' 有一条对应边的长度不同，矛盾！如果 + 和 − 都有，那么有一条两条边中点的“分界线”把所有 + 和 − 分离 (因为只有两次符号变化). 再用下面的引理，我们可以推出矛盾. □

Cauchy 的手臂引理.

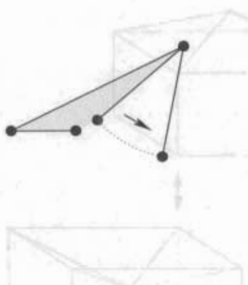
如果 Q 和 Q' 都是凸 (平面或球面) n 边形，如图所示来标记，



使得对于 $1 \leqslant i \leqslant n-1$ 有对应边的长度 $\overline{q_iq_{i+1}} = \overline{q'_iq'_{i+1}}$ 成立，并且对于 $2 \leqslant i \leqslant n-1$ 有对应角的大小 $\alpha_i \leqslant \alpha'_i$. 那么那个“剩下的”边的长度满足

$$\overline{q_1q_n} \ \leqslant \ \overline{q'_1q'_n},$$

等号成立当且仅当对所有 $2 \leqslant i \leqslant n-1$, $\alpha_i = \alpha'_i$ 都成立.



有趣的是，Cauchy 原来对于引理的证明是错误的：一个保持边长不变和打开的角连续的运动有可能会丢失凸性 —— 见图！另一方面，从 I. J. Schoenberg 给 S. K. Zaremba 的信中得到的引理和它的证明对平面和球面的多面体都是成立的.

■ **证明.** 我们对 n 用归纳法. $n=3$ 的情况很简单：如果在一个三角形中增加两条长度固定为 a 和 b 的边的夹角 γ，那么对边的长度 c 也会增加. 这可由如下公式推出：平面情形的余弦定理

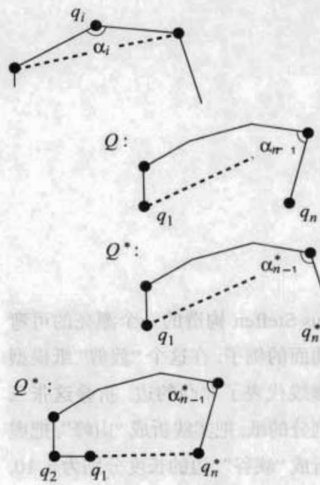
$$c^2 \ = \ a^2 + b^2 - 2ab\cos\gamma$$

和球面三角形的相似结果

$$\cos c \ = \ \cos a \cos b + \sin a \sin b \cos\gamma,$$

这里长度 a, b, c 都是在单位球的表面上量得的，从而它们的值在 $[0, \pi]$ 之间.

现在令 $n \geqslant 4$. 如果对某个 $i \in \{2, \cdots, n-1\}$ 我们有 $\alpha_i = \alpha'_i$, 那么对应点可以被从 q_{i-1} 到 q_{i+1}, 以及从 q'_{i-1} 到 q'_{i+1} 的对角线被分割成两个角, 由于有 $\overline{q_{i-1}q_{i+1}} = \overline{q'_{i-1}q'_{i+1}}$, 由归纳假设完成了证明. 所以我们可以假定对于 $2 \leqslant i \leqslant n-1$, 都有 $\alpha_i < \alpha'_i$.



下面我们从 Q 出发作新的图 Q^*: 我们把 Q 中的 α_{n-1} 用使 Q^* 保持凸性且满足 $\alpha^*_{n-1} \leqslant \alpha'_{n-1}$ 的最大可能的角 α^*_{n-1} 来代替. 这时, 我们用 q^*_n 代替 q_n, 保持 Q 的其他 q_i 和边长、角度不变.

如果我们确定能选择 $\alpha^*_{n-1} = \alpha'_{n-1}$ 且保持 Q^* 的凸性, 则有

$$\overline{q_1q_n} < \overline{q_1q^*_n} \leqslant \overline{q'_1q'_n},$$

其中的第一步用到了 $n = 3$ 的情形, 第二步用到上面的归纳假设.

否则经过一个非平凡的移动后可得到

$$\overline{q_1q^*_n} > \overline{q_1q_n}, \tag{1}$$

我们被卡在了 q_2, q_1 和 q^*_n 共线的情形, 此时

$$\overline{q_2q_1} + \overline{q_1q^*_n} = \overline{q_2q^*_n}. \tag{2}$$

现在我们比较 Q^* 和 Q'. 由对 n 的归纳 (忽略顶点 q_1 和 q'_1) 可以发现

$$\overline{q_2q^*_n} \leqslant \overline{q'_2q'_n}. \tag{3}$$

因此我们有

$$\overline{q'_1q'_n} \overset{(*)}{\geqslant} \overline{q'_2q'_n} - \overline{q'_1q'_2} \overset{(3)}{\geqslant} \overline{q_2q^*_n} - \overline{q_1q_2} \overset{(2)}{=} \overline{q_1q^*_n} \overset{(1)}{>} \overline{q_1q_n},$$

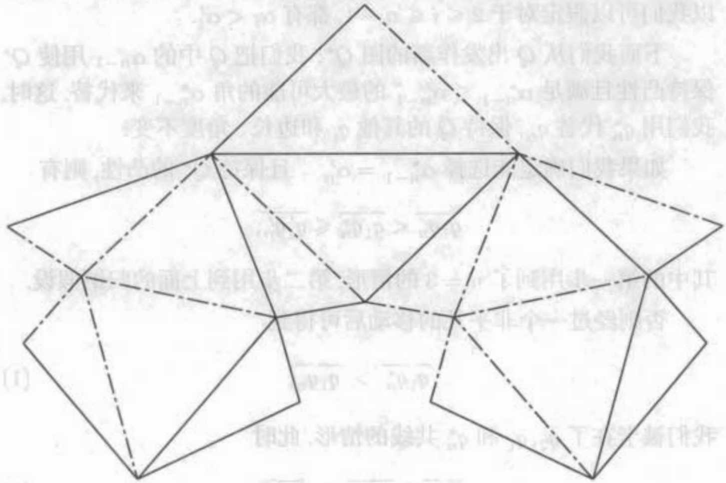
其中 $(*)$ 只是三角不等式, 而其他关系已经推出. □

我们已经见过一个例子表明 Cauchy 刚性定理对于非凸多面体不成立. 当然这个例子的特点是: 有一个从一个多面体到另一个多面体的不连续的 "突变", 保持了多面体所有的对应面全等而二面角跳跃式突然变动. 所以我们可进一步地问:

> 对于某个非凸多面体是否有一个连续变换保持各个面的平面性和全等性?

人们推测没有可三角剖分的面, 无论是不是凸的, 允许这样一种变换. 所以, Robert Connelly 在 1977 年 ——Cauchy 的工作出现 160

多年以后,举出的以下反例是十分让人吃惊的: 被镶嵌在 $\mathbb{R}^3$ 中的闭合的可三角剖分的球面 (没有自相交), 通过一个连续的保持边长不变并保持三角形的面全等的变化是可以弯曲的.



Klaus Steffen 构造的一个漂亮的可弯曲曲面的例子: 在这个 "裁剪" 纸模型中虚线代表了非凸的边. 折叠这张三角剖分的纸, 把实线折成 "山峰", 把虚线折成 "峡谷". 边的长度分别为 5, 10, 11, 12 和 17 个单位.

Cauchy 刚性定理蕴藏了更加令人吃惊的结论: 直到最近才由 Connelly, Sabitov 和 Walz 证明了当任意一个这样的可弯曲曲面运动时, 它围出的多边体的体积不变. 他们的证明本身也是漂亮的, 用到了代数工具 (超出了本书的范围).

参考文献

[1] A. Cauchy: *Sur les polygones et les polyèdres, seconde mémoire,* J. École Polytechnique XVIe Cahier, Tome IX (1813), 87-98; Œuvres Complètes, IIe Série, Vol. 1, Paris 1905, 26-38.

[2] R. Connelly: *A counterexample to the rigidity conjecture for polyhedra,* Inst. Haut. Etud. Sci., Publ. Math. **47** (1978), 333-338.

[3] R. Connelly: *The rigidity of polyhedral surfaces,* Mathematics Magazine **52** (1979), 275-283.

[4] I. Kh. Sabitov: *The volume as a metric invariant of polyhedra,* Discrete Comput. Geometry. **20** (1998), 405-425.

[5] J. Schoenberg & S.K. Zaremba: *On Cauchy's lemma concerning convex polygons,* Canadian J. Math. **19** (1967), 1062-1071.

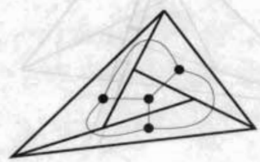
第 13 章

相切单纯形

多少个 d 维单纯形可以被放在 $\mathbb{R}^d$ 中，使得它们两两相切，也就是说，它们两两之间的交是 $(d-1)$ 维的？

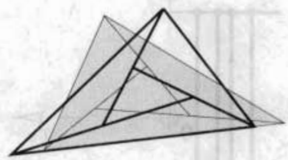
这是一个古老而又自然的问题. 我们把这个问题的答案记作 $f(d)$，显然我们有 $f(1) = 2$. 对于 $d = 2$，如边图的四个三角形组成的图形表明 $f(2) \geqslant 4$. 由五个三角形组成的两两相切的图形是不存在的，否则它的对偶图便是一个 K_5 的平面嵌入，由前面的章节我们知道这是不可能的. 图中那个有 4 个三角形的例子就得到了 K_4 的一个平面画法. 从而

$$f(2) = 4.$$



$f(2) \geqslant 4$

三维的情况下，很显然有 $f(3) \geqslant 8$. 如边图的 8 个三角形便说明了这一点. 阴影部分的四个三角形连接着“画出的平面”下方的某一个点 x，这提供了在此平面下方且与此平面相切的四个四面体. 同样地，四个白色的三角形连接该平面上方的一个点 y. 这样我们就得到了 $\mathbb{R}^3$ 中的八个两两相切的四面体，从而，$f(3) \geqslant 8$.



$f(3) \geqslant 8$

1965 年，Baston在一本著作中证明了 $f(3) \leqslant 9$，Zaks于 1991 年在另一本书中证明了

$$f(3) = 8.$$

既然有了 $f(1) = 2, f(2) = 4$ 以及 $f(3) = 8$，自然地便有了如下推测，这个推测最早由Bagemihl在 1956 年给出.

猜想. 在 $\mathbb{R}^d$ 中，最多有

$$f(d) = 2^d$$

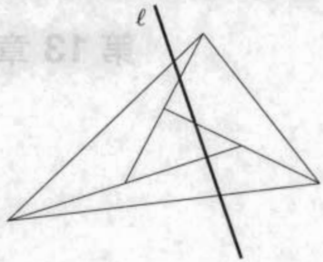
个 d 维单纯形两两相切.

通过合理的构造，我们不难得到下界 $f(d) \geqslant 2^d$. 这些构造用到了仿射坐标变换，并且由 Joseph Zaks [4] 利用对维数的归纳推出了以下更强的结论.

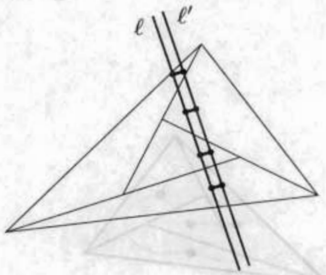
定理 1. 对于每个 $d \geqslant 2$，在 $\mathbb{R}^d$ 中有一族 2^d 个两两相切的 d- 单纯形，并且存在一条直线经过每个单纯形的内部.



“相切单纯形”



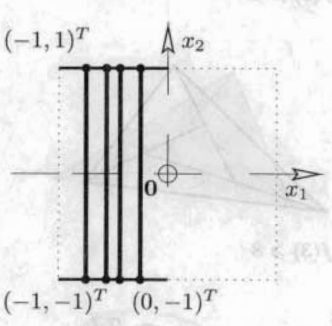
■ **证明.** 对于 $d = 2$ 的情况, 我们考虑过的那个含 4 个三角形的族确实存在这样一条直线经过每个三角形的内部. 现在考虑任何两两相切并且有一条直线 ℓ 经过的 d 维单纯形. 任何与 ℓ 足够接近的直线 ℓ' 也经过了每个单纯形. 如果我们选择 ℓ' 与 ℓ 平行并且足够接近, 那么在每个单纯形内部都有这两条平行线之间的与之垂直的 (最短) 连接线段. 直线 ℓ 和 ℓ' 只有有限制的部分在每个单纯形内部, 从而我们可以在此构形外面添加两条连接线段, 使得由这两条外部的连接线张成的矩形 (即它们的凸包) 包含了所有其他的连接线段. 这样, 我们得到了一个 "梯子", 使得每个单纯形都有此梯子的一个梯阶在它的内部, 而梯子的 4 个端点在所有单纯形的外部.



现在主要步骤便是通过一个 $\mathbb{R}^d$ 到 $\mathbb{R}^d$ 的 (仿射) 坐标变换把由梯子围成的矩形变换到如下所给出的矩形 (半正方形):

$$R^1 \;=\; \{(x_1, x_2, 0, \cdots, 0)^T : -1 \leqslant x_1 \leqslant 0; -1 \leqslant x_2 \leqslant 1\}.$$

从而我们得到 $\mathbb{R}^d$ 中由这些单纯形组成的构形 (记为 Σ^1), x_1- 轴穿过它的每个单纯形的内部, 并且每个单纯形包含了此直线上的线段



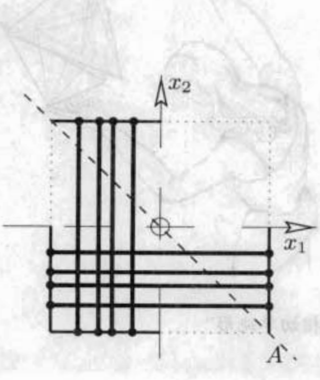
$$S^1(\alpha) \;=\; \{(\alpha, x_2, 0, \cdots, 0)^T : -1 \leqslant x_2 \leqslant 1\}$$

在其内部 (对某个满足 $-1 < \alpha < 0$ 的 α), 而原点 $\mathbf{0}$ 在所有单纯形的外部.

现在我们通过把第一个构形作关于由 $x_1 = x_2$ 给定的超平面的反射得到第二个构形 Σ^2. x_2- 轴经过了 Σ^2 的每个单纯形的内部, 并且每个单纯形包含线段

$$S^2(\beta) \;=\; \{(x_1, \beta, 0, \cdots, 0)^T : -1 \leqslant x_1 \leqslant 1\}$$

在其内部, 其中 $-1 < \beta < 0$. 但是每条线段 $S^1(\alpha)$ 与每条线段 $S^2(\beta)$ 相交, 从而 Σ^1 的每个单纯形内部与 Σ^2 的每个单纯形内部相交. 如果我们增加一个新的坐标 x_{d+1}, 并且令 Σ 为



$$\{\mathrm{conv}(P_i \cup \{-\boldsymbol{e}_{d+1}\}) : P_i \in \Sigma^1\} \,\cup\, \{\mathrm{conv}(P_j \cup \{\boldsymbol{e}_{d+1}\}) : P_j \in \Sigma^2\},$$

那么我们得到 $\mathbb{R}^{d+1}$ 中的一个两两相切 $(d+1)$- 单纯形的构形.

进一步, 反对角线

$$A \;=\; \{(x, -x, 0, \cdots, 0)^T : x \in \mathbb{R}\} \;\subseteq\; \mathbb{R}^d$$

与每个 $S^1(\alpha)$ 和 $S^2(\beta)$ 中线段相交. 我们把它 "倾斜" 一点, 得到一

条直线

$$L_\varepsilon \;=\; \{(x,-x,0,\cdots,0,\varepsilon x)^T : x\in\mathbb{R}\} \subseteq \mathbb{R}^{d+1},$$

对于所有足够小的 $\varepsilon > 0$, 这条直线与 Σ 的每个单纯形相交. 这样便完成了我们的归纳. □

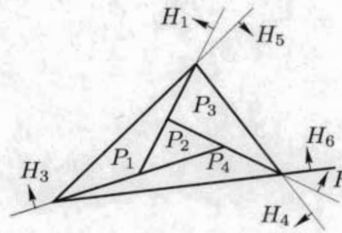
与这个指数下界截然相反, 紧的上界却很难得到. 一个简单的归纳推导只能得到 (分别考虑一个相切的构形中的所有超平面)

$$f(d) \;\leqslant\; \frac{2}{3}(d+1)!,$$

这离定理 1 给出的下界要差很多. 然而, Micha Perles发现了一个 "神奇" 的证明方法将这个上限大大降低.

定理 2. 对所有 $d \geqslant 1$ 我们有 $f(d) < 2^{d+1}$.

■ **证明.** 在 $\mathbb{R}^d$ 中给定 r 个两两相切的 d- 单纯形 $P_1, P_2, \cdots, P_r$, 首先列举出由 P_i 的面张成的不同超平面 $H_1, H_2, \cdots, H_s$, 对每个超平面任意选择一个正面 H_i^+, 称它的另一面为反面 H_i^-.



例如, 对于二维的 $r = 4$ 个三角形, 如边图所示我们得到 $s = 6$ 个超平面 (当 $d = 2$ 时它们是边).

由这些数据, 我们构造一个B- 矩阵: 它是一个 $(r \times s)$- 矩阵, 每个元素如下取自 $\{+1, -1, 0\}$:

$$B_{ij} := \begin{cases} +1, & \text{如果}P_i\text{ 有一个面在}H_j\text{中, 并且}P_i \subseteq H_j^+, \\ -1, & \text{如果}P_i\text{ 有一个面在}H_j\text{中, 并且}P_i \subseteq H_j^-, \\ 0, & \text{如果}P_i\text{ 没有面在}H_j\text{中.} \end{cases}$$

例如, 边图的二维构形得到矩阵

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ -1 & -1 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 \end{pmatrix}.$$

这样的 B- 矩阵有三个值得注意的性质. 首先, 因为每个 d- 单纯形有 $d+1$ 个面, 我们发现 B 的每一行有恰好 $d+1$ 个非零的元素, 从而有 $s-(d+1)$ 个零元素. 第二, 由于每两个单纯形是相切的, 从而对任意两行一定有一列其元素在其中的一行是 $+1$, 在另一行是 -1. 也就是说, 即使我们不考虑零元素这些行也是互不相同的. 第三, B 的每一行通过

$$P_i \;=\; \bigcap_{j:B_{ij}=1} H_j^+ \;\cap \bigcap_{j:B_{ij}=-1} H_j^- . \qquad (*)$$

“代表” 了一个单纯形 P_i. 现在我们从 B 得到一个新矩阵 C, 其中 B 的每一行被替换成把这一行的零元素变成 $+1$ 或 -1 的所有可能的行. 既然 B 的每一行有 $s-d-1$ 个零元素, 并且 B 有 r 行, 矩阵 C 有 $2^{s-d-1}r$ 行.

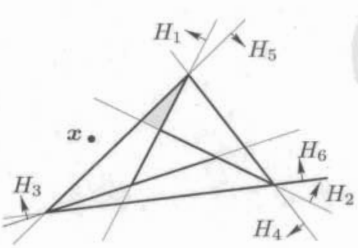
在我们的例子中, 矩阵 C 是一个 (32×6)- 矩阵, 前几行是

$$C=\left(\begin{array}{cccccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ \hline -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}\right),$$

C 的前八行由 B 的第一行得到, 接下来的八行由 B 的第二行得到, 等等.

现在的关键是 C 的任意两行都是不同的: 如果这两行是从 B 的同一行生成的, 那么原来的零元素被不同的元素代替; 如果这两行是从 B 的不同行生成的, 那么在 B 的非零元素处它们便是不同的. 但是 C 的行是长为 s 的 (±1)- 向量, 而只有 2^s 个不同的这样的向量. 由于 C 的行互不相同从而 C 最多有 2^s 行, 也就是说,

$$2^{s-d-1}r \leqslant 2^s.$$



C- 矩阵的第一行代表了阴影中的三角形, 第二行对应了一个半平面的空的交集. 点 x 对应了一个不出现在 C- 矩阵中的向量 $(1,-1,1,1,-1,1)$.

然而, 不可能所有的 (±1)- 向量都出现在 C 中, 这可导出严格不等式 $2^{s-d-1}r<2^s$, 进而 $r<2^{d+1}$. 为了说明这点, 我们注意到 C 的每一行代表了半空间的相交 —— 正如同 B 的行通过公式 $(*)$ 一样. 这个交集是单纯形 P_i 的对应于 B 相应行的子集. 我们选一点 $x\in\mathbb{R}^d$ 不在任意超平面 H_j 上, 也不在任意单纯形 P_i 中. 从这个点 x 我们得到一个 (±1)- 向量记录了对每个 j 是有 $x\in H_j^+$ 还是 $x\in H_j^-$. 这个 (±1)- 向量就不出现在 C 中 (因为根据 $(*)$ 它代表的半空间的交集包含 x, 从而不被任一单纯形 P_i 包含). □

参考文献

[1] F. Bagemihl: *A conjecture concerning neighboring tetrahedra,* Amer. Math. Monthly **63** (1956) 328-329.

[2] V. J. D. Baston: *Some Properties of Polyhedra in Euclidean Space,* Pergamon Press, Oxford 1965.

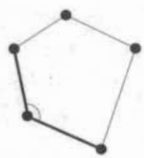
[3] M. A. Perles: *At most* 2^{d+1} *neighborly simplices in* E^{d}, Annals of Discrete Math. **20** (1984), 253-254.

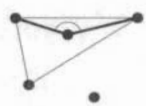
[4] J. Zaks: *Neighborly families of* 2^{d} *d-simplices in* E^{d}, Geometriae Dedicata **11** (1981), 279-296.

[5] J. Zaks: *No Nine Neighborly Tetrahedra Exist,* Memoirs Amer. Math. Soc. No. 447, Vol. 91, 1991.

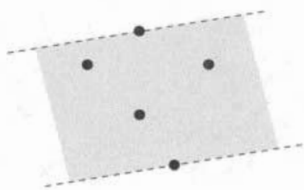
每一个足够大的点集都会生成钝角　第 14 章

1950 年左右, Paul Erdős提出了如下猜测: $\mathbb{R}^d$ 上的每个大于 2^d 个点的集合一定会产生至少一个钝角, 也就是说, 一个严格大于 $\frac{\pi}{2}$ 的角. 换句话说, 任何在 $\mathbb{R}^d$ 上不产生钝角的点集最多包含 2^d 个点. 这个问题被荷兰数学会列为 "有奖征答" 问题, 但是只得到了 $d=2$ 和 $d=3$ 时的答案.





对于 $d=2$ 这个问题很简单: 如果五个点形成了一个凸五边形, 那么总是有钝角 (事实上, 至少有一个内角会大于等于 108°). 否则, 我们总有一个点被包含在一个三个点组成的三角形里面. 但这个点能通过以其为顶点的和为 360° 的三个角 "看见" 这个三角形的三条边, 从而一定有其中一个角大于等于 120°. (这第二种情况也包含了三点共线的情况, 从而有角度 180°).



与这个猜想不相关的另一个问题由Victor Klee在几年之后提出, 并且由Erdős扩展. 这个问题即在 $\mathbb{R}^d$ 中多大的点集还能保持下面的 "对径" 性质: 对点集中的任意两个点, 都存在一条带子 (由两个平行的超平面作边界) 包含了点集, 并且这两个选定的点分别在两个超平面上.

在 1962 年, Ludwig Danzer和Branko Grünbaum同时解决了这两个问题: 这两个问题的上限和下限都是 2^d. 从而 2^d 同时是这两个问题的答案.

接下来, 我们考虑 (有限) 点集 $S \subseteq \mathbb{R}^d$, 它的凸包是 $\text{conv}(S)$, 以及凸多胞体 $Q \subseteq \mathbb{R}^d$ (参见第 8 章有关多胞体基本定义的附录). 假设这些点集是 d 维的, 也就是说, 它们不被任何一个超平面包含. 称两个凸集**接触**, 如果它们至少有一个共同的边界点, 而它们的内部没有交集. 对任何集合 $Q \subseteq \mathbb{R}^d$ 和任何向量 $\boldsymbol{s} \in \mathbb{R}^d$, 我们记 $Q+\boldsymbol{s}$ 为平移体 $\{x+\boldsymbol{s} : x \in Q\}$, 类似地, $Q-\boldsymbol{s}$ 为平移体 $\{x-\boldsymbol{s} : x \in Q\}$.

不用担心, 这一章是到 d 维几何的一次漫步, 下面的论证并不需要 "高维几何想象". 因为它们都可以通过三维空间甚至二维平面来图示 (因此可以理解). 所以, 我们的几何图将演示二维的情况 (此时的 "超平面" 就是一条直线), 你可以类似地画出 $d=3$ 的图 (此时

的“超平面”是一个平面).

定理 1. 对每个 d, 我们有下面一串不等式:

$$2^d \overset{(1)}{\leqslant} \max\left\{\#S \,\middle|\, \begin{array}{l} S\subseteq\mathbb{R}^d, \text{对任意的 } \{\boldsymbol{s}_i,\boldsymbol{s}_j,\boldsymbol{s}_k\}\subseteq S \text{ 有 } \sphericalangle(\boldsymbol{s}_i,\boldsymbol{s}_j,\\ \boldsymbol{s}_k)\leqslant\frac{\pi}{2}\end{array}\right\}$$

$$\overset{(2)}{\leqslant} \max\left\{\#S \,\middle|\, \begin{array}{l} S\subseteq\mathbb{R}^d \text{使得对任意两个点 } \{\boldsymbol{s}_i,\boldsymbol{s}_j\}\subseteq S \text{ 有一条}\\ \text{带子 } \mathcal{S}(i,j) \text{ 包含 } S, \text{并且 } \boldsymbol{s}_i \text{ 和 } \boldsymbol{s}_j \text{ 分别在这条带}\\ \text{子的两侧}\end{array}\right\}$$

$$\overset{(3)}{=} \max\left\{\#S \,\middle|\, \begin{array}{l} S\subseteq\mathbb{R}^d \text{使得凸包 } P:=\mathrm{conv}(S) \text{ 的平移体 } P-\boldsymbol{s}_i,\\ \boldsymbol{s}_i\in S \text{ 交于同一个点, 但仅仅是接触}\end{array}\right\}$$

$$\overset{(4)}{\leqslant} \max\left\{\#S \,\middle|\, \begin{array}{l} S\subseteq\mathbb{R}^d \text{使得对于某个 } d \text{ 维凸多胞体 } Q\subseteq\mathbb{R}^d \text{ 的}\\ \text{平移体 } Q+\boldsymbol{s}_i \text{ 两两接触}\end{array}\right\}$$

$$\overset{(5)}{=} \max\left\{\#S \,\middle|\, \begin{array}{l} S\subseteq\mathbb{R}^d \text{使得对于某个 } d \text{ 维中心对称凸多胞}\\ \text{体 } Q^*\subseteq\mathbb{R}^d \text{ 的平移体 } Q^*+\boldsymbol{s}_i \text{ 两两接触}\end{array}\right\}$$

$$\overset{(6)}{\leqslant} 2^d.$$

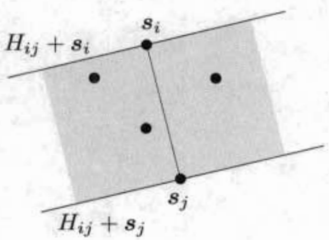
■ **证明.** 我们有六个断言 (等式及不等式) 需要证明.

(1) 令 $S:=\{0,1\}^d$ 是 $\mathbb{R}^d$ 中标准单位立方体的顶点集, 选择 $\boldsymbol{s}_i,\boldsymbol{s}_j,\boldsymbol{s}_k\in S$. 由对称性我们不妨假设 $\boldsymbol{s}_j=\boldsymbol{0}$ 是零向量. 从而角度可以如下计算:

$$\cos\sphericalangle(\boldsymbol{s}_i,\boldsymbol{s}_j,\boldsymbol{s}_k)=\frac{\langle\boldsymbol{s}_i,\boldsymbol{s}_k\rangle}{|\boldsymbol{s}_i||\boldsymbol{s}_k|},$$

这显然是非负的. 从而 S 有 $|S|=2^d$ 并且没有钝角.

(2) 如果 S 没有钝角, 那么对于任意 $\boldsymbol{s}_i,\boldsymbol{s}_j\in S$ 我们可以定义 $H_{ij}+\boldsymbol{s}_i$ 和 $H_{ij}+\boldsymbol{s}_j$ 为平行的分别经过 $\boldsymbol{s}_i$ 和 $\boldsymbol{s}_j$ 的超平面, 并且这两个超平面与边 $[\boldsymbol{s}_i,\boldsymbol{s}_j]$ 垂直. 这里



$$H_{ij}=\{\boldsymbol{x}\in\mathbb{R}^d\colon \langle\boldsymbol{x},\boldsymbol{s}_i-\boldsymbol{s}_j\rangle=0\}$$

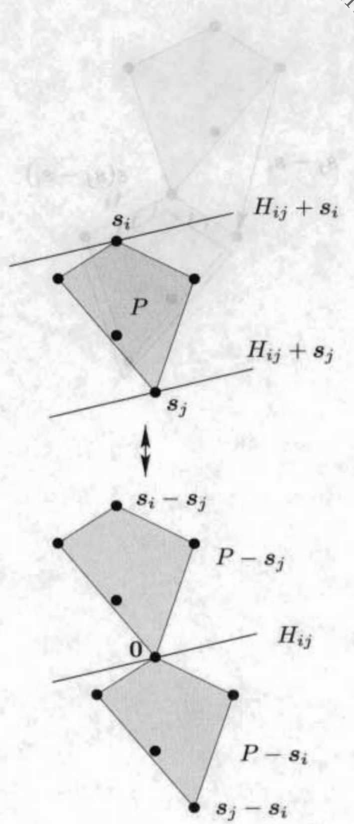
是经过原点的垂直于边 $[\boldsymbol{s}_i,\boldsymbol{s}_j]$ 的超平面, 并且 $H_{ij}+\boldsymbol{s}_j=\{\boldsymbol{x}+\boldsymbol{s}_j:\boldsymbol{x}\in H_{ij}\}$ 是经过 $\boldsymbol{s}_j$ 的 H_{ij} 的平移体. 从而 $H_{ij}+\boldsymbol{s}_i$ 和 $H_{ij}+\boldsymbol{s}_j$ 之间的带子包含有 $\boldsymbol{s}_i$ 和 $\boldsymbol{s}_j$ 以及使得 $\sphericalangle(\boldsymbol{s}_i,\boldsymbol{s}_j,\boldsymbol{x})$ 和 $\sphericalangle(\boldsymbol{s}_j,\boldsymbol{s}_i,\boldsymbol{x})$ 都不是钝角的所有点 $\boldsymbol{x}\in\mathbb{R}^d$. 从而这条带子包含 S 的全部.

(3) P 被 $H_{ij}+\boldsymbol{s}_j$ 的包含 $\boldsymbol{s}_i$ 的半空间包含当且仅当 $P-\boldsymbol{s}_j$ 被 H_{ij} 的包含 $\boldsymbol{s}_i-\boldsymbol{s}_j$ 的半空间包含: 如果我们以同样的尺度值 (即 $-\boldsymbol{s}_j$) 同时平移对象和半空间, 则不会改变“对象包含在半空间中”的性

质. 相似地, P 被 $H_{ij}+\boldsymbol{s}_i$ 的包含 $\boldsymbol{s}_j$ 的半空间包含当且仅当 $P-\boldsymbol{s}_i$ 被 H_{ij} 的包含 $\boldsymbol{s}_j-\boldsymbol{s}_i$ 的半空间包含.

将这些性质放在一起, 我们发现多胞体 P 包含在以 $H_{ij}+\boldsymbol{s}_i$ 和 $H_{ij}+\boldsymbol{s}_j$ 为边界的带子中当且仅当 $P-\boldsymbol{s}_i$ 和 $P-\boldsymbol{s}_j$ 在 H_{ij} 超平面的不同半空间中.

这一对应由旁边的图所示.



进一步, 从 $\boldsymbol{s}_i\in P=\operatorname{conv}(S)$ 我们有原点 $\mathbf{0}$ 被包含在所有平移体 $P-\boldsymbol{s}_i\ (\boldsymbol{s}_i\in S)$ 中. 从而我们可以看到这些集合 $P-\boldsymbol{s}_i$ 交在 $\mathbf{0}$, 但它们只是接触: 由于它们在对应超平面 H_{ij} 的不同侧, 它们的内部互不相交.

(4) 这个我们很容易得到: "平移体两两接触" 要弱于 "它们交在同一个点, 并且它们只是接触." 相似地, 我们可以减弱条件, 设 P 为任意一个 $\mathbb{R}^d$ 中的凸的d- 多胞体. 更进一步, 我们也许可以用 $-S$ 代替 S.

(5) 这里 "$\geqslant$" 是平凡的, 但这一点并不是我们感兴趣的方向. 我们必须从构形 $S\subseteq\mathbb{R}^d$ 和任意一个 d- 多胞体 $Q\subseteq\mathbb{R}^d$ 入手使得平移体 $Q+\boldsymbol{s}_i\ (\boldsymbol{s}_i\in S)$ 两两接触. 我们断言这时可以用

$$Q^*:=\left\{\tfrac{1}{2}(\boldsymbol{x}-\boldsymbol{y})\in\mathbb{R}^d:\boldsymbol{x},\boldsymbol{y}\in Q\right\}$$

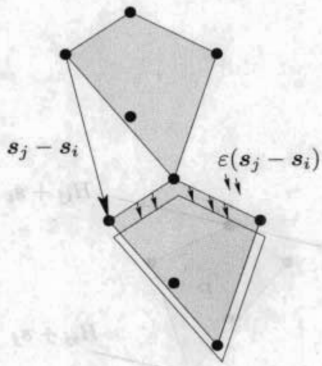
代替 Q. 这不难验证: 首先, Q^* 是 d 维的, 凸的, 中心对称的. Q^* 一定是一个多胞体 (它的顶点为 $\frac{1}{2}(\boldsymbol{q}_i-\boldsymbol{q}_j)$, 其中 $\boldsymbol{q}_i,\boldsymbol{q}_j$ 是 Q 的顶点), 但这对我们并不重要.

现在我们要证明 $Q+\boldsymbol{s}_i$ 和 $Q+\boldsymbol{s}_j$ 相接触当且仅当 $Q^*+\boldsymbol{s}_i$ 和 $Q^*+\boldsymbol{s}_j$ 接触. 为此我们跟随Minkowski注意到,

$$\begin{aligned}
&(Q^*+\boldsymbol{s}_i)\cap(Q^*+\boldsymbol{s}_j)\neq\varnothing\\
&\quad\Longleftrightarrow\ \exists\,\boldsymbol{q}_i',\boldsymbol{q}_i'',\boldsymbol{q}_j',\boldsymbol{q}_j''\in Q:\tfrac{1}{2}(\boldsymbol{q}_i'-\boldsymbol{q}_i'')+\boldsymbol{s}_i=\tfrac{1}{2}(\boldsymbol{q}_j'-\boldsymbol{q}_j'')+\boldsymbol{s}_j\\
&\quad\Longleftrightarrow\ \exists\,\boldsymbol{q}_i',\boldsymbol{q}_i'',\boldsymbol{q}_j',\boldsymbol{q}_j''\in Q:\tfrac{1}{2}(\boldsymbol{q}_i'+\boldsymbol{q}_j'')+\boldsymbol{s}_i=\tfrac{1}{2}(\boldsymbol{q}_j'+\boldsymbol{q}_i'')+\boldsymbol{s}_j\\
&\quad\Longleftrightarrow\ \exists\,\boldsymbol{q}_i,\boldsymbol{q}_j\in Q:\boldsymbol{q}_i+\boldsymbol{s}_i=\boldsymbol{q}_j+\boldsymbol{s}_j\\
&\quad\Longleftrightarrow\ (Q+\boldsymbol{s}_i)\cap(Q+\boldsymbol{s}_j)\neq\varnothing,
\end{aligned}$$

其中在第三个 (重要的) "$\Longleftrightarrow$" 时我们用到每个 $\boldsymbol{q}\in Q$ 可以被写成 $\boldsymbol{q}=\frac{1}{2}(\boldsymbol{q}+\boldsymbol{q})$ 来得到 "$\Leftarrow$", 并且 Q 是凸的, 从而得到 $\frac{1}{2}(\boldsymbol{q}_i'+\boldsymbol{q}_j''),\frac{1}{2}(\boldsymbol{q}_j'+\boldsymbol{q}_i'')\in Q$. 这样也就得到 "$\Rightarrow$".

从而 Q 到 Q^* 的道路 (被称为 *Minkowski* 对称) 保留了两个平移体 $Q+\boldsymbol{s}_i$ 和 $Q+\boldsymbol{s}_j$ 相交的性质. 也就是说, 我们证明了对于任意凸



集 Q, 两个平移体 $Q+s_i$ 和 $Q+s_j$ 相交当且仅当 Q^*+s_i 和 Q^*+s_j 相交.

下面的性质表明 Minkowski 对称还保持了两个平移接触的性质:

> $Q+s_i$ 和 $Q+s_j$ 接触当且仅当它们相交, 然而对任意 $\varepsilon>0$, $Q+s_i$ 和 $Q+s_j+\varepsilon(s_j-s_i)$ 不交.

(6) 假设 Q^*+s_i 和 Q^*+s_j 接触. 对每个交点

$$x \in (Q^*+s_i)\cap(Q^*+s_j),$$

我们有

$$x-s_i \in Q^* \quad \text{和} \quad x-s_j \in Q^*,$$

所以, 因为 Q^* 是中心对称的,

$$s_i - x = -(x-s_i) \in Q^*,$$

进而, 由于 Q^* 是凸的,

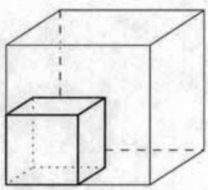
$$\tfrac{1}{2}(s_i-s_j)=\tfrac{1}{2}\left((x-s_j)+(s_i-x)\right)\in Q^*.$$

对任意 i, 我们得到 Q^*+s_j 包含 $\frac{1}{2}(s_i+s_j)$. 这样, 对于 $P:=\mathrm{conv}(S)$ 我们有

$$P_j := \tfrac{1}{2}(P+s_j)=\mathrm{conv}\left\{\tfrac{1}{2}(s_i+s_j) : s_i \in S\right\}\subseteq Q^*+s_j,$$

从而 $P_j=\frac{1}{2}(P+s_j)$ 只能相接触.

最后, 因为所有点 s_i, s_j 和 $\frac{1}{2}(s_i+s_j)$ 都在 P 中, 集合 P_j 被包含在 P 中 (P 是凸的). 但是 P_j 是将 P 按比例缩小且又包含在 P 中的一些平移体. 所以当缩小比例为 $\frac{1}{2}$ 时



缩小比例为 $\frac{1}{2}$, 这时 $\mathrm{vol}(P_j)=\frac{\mathrm{vol}(P)}{8}$

$$\mathrm{vol}(P_j) \;=\; \frac{1}{2^d}\mathrm{vol}(P),$$

因为我们在处理 d 维的点集. 这也意味着最多有 2^d 个集合 P_j 能恰好装入 P 中, 从而 $|S|\leqslant 2^d$.

这样便完成这串不等式的证明. □

…… 故事还没有结束. Danzer 和 Grünbaum 提出了下列问题:

> 如果要求所有的角是锐角, 而不只是非钝角, 也就是不允许直角, 会怎么样?

他们构造了 $\mathbb{R}^d$ 中的 $2d-1$ 个只生出锐角的点，想证明这样是最好的情况. Grünbaum证明这对于 $d \leqslant 3$ 确实成立. 但是仅仅 21 年之后，在 1983 年，Paul Erdős 和 Zoltan Füredi 证明了如果维数较高则这个猜想是错的! 很有戏剧性. 他们的证明是显示概率论方法威力的极好例证，参见第 35 章中对于 "概率方法" 的介绍. 我们的证明利用了读者 David Bevan 给出的比原来更好的参数设置.

定理 2. 对每个 $d \geqslant 2$，存在 $\mathbb{R}^d$ 中 $2\lfloor\frac{\sqrt{6}}{9}\big(\frac{2}{\sqrt{3}}\big)^d\rfloor$ 个点的点集 $S \subseteq \{0,1\}^d$(单位 d- 立方体的顶点) 使得这些点只决定锐角. 特别地，当维数 $d=34$ 时有一个 $72 > 2\cdot 34-1$ 个点的点集只决定锐角.

■ **证明.** 令 $m := \lfloor\frac{\sqrt{6}}{9}\big(\frac{2}{\sqrt{3}}\big)^d\rfloor$，任意挑选 $3m$ 个向量

$$\boldsymbol{x}(1), \boldsymbol{x}(2), \cdots, \boldsymbol{x}(3m) \in \{0,1\}^d$$

使得它们的坐标为 0 或者 1 并且是独立和随机的，两种的概率各为 $\frac{1}{2}$. (你可以将一个银币投掷 $3md$ 次; 然而，如果 d 很大，你很快就会厌烦.)

由上面可知每个由 0/1- 向量决定的角度都不是钝角. 三个向量 $\boldsymbol{x}(i), \boldsymbol{x}(j), \boldsymbol{x}(k)$ 共同决定了一个直角顶点 $\boldsymbol{x}(j)$ 当且仅当标量积 $\langle \boldsymbol{x}(i)-\boldsymbol{x}(j), \boldsymbol{x}(k)-\boldsymbol{x}(j)\rangle$ 为 0，也就是，如果对每个坐标 ℓ 有 $x(i)_\ell - x(j)_\ell = 0$ 或 $x(k)_\ell - x(j)_\ell = 0$. 此时，我们称 (i,j,k) 是一个坏的三元集. (如果 $\boldsymbol{x}(i) = \boldsymbol{x}(j)$ 或者 $\boldsymbol{x}(j) = \boldsymbol{x}(k)$，那么角度是不定的，从而 (i,j,k) 当然是坏的)

一个特定三元集是坏的概率是 $\big(\frac{3}{4}\big)^d$: 事实上，它是好的当且仅当，对某个 d 坐标 ℓ，我们有

$$\begin{aligned}
&\text{或者}\quad x(i)_\ell = x(k)_\ell = 0, \quad x(j)_\ell = 1,\\
&\text{或者}\quad x(i)_\ell = x(k)_\ell = 1, \quad x(j)_\ell = 0.
\end{aligned}$$

这让我们在 8 种可能性中有 6 个坏的选择. 而一个三元集是坏的当且仅当对于每个 d 坐标做出了坏的选择 (以 $\frac{3}{4}$ 的概率).

我们要考虑的三元集的个数是 $3\binom{3m}{3}$，这是由于共有 $\binom{3m}{3}$ 个三元集，并且对于每个的顶点有三种选择. 当然，不同三元集是坏的事件是不独立的: 但是期望的线性性 (即对所有可能选择取平均，见附录) 得出坏三元集的期望是 $3\binom{3m}{3}\big(\frac{3}{4}\big)^d$. 这意味着 —— 也是概率方法显示威力的地方 —— 一定有某个选择使得最多 $3\binom{3m}{3}\big(\frac{3}{4}\big)^d$ 个三元集是坏的，其中通过 m 的选择

$$3\binom{3m}{3}\Big(\frac{3}{4}\Big)^d < 3\frac{(3m)^3}{6}\Big(\frac{3}{4}\Big)^d = m^3\Big(\frac{9}{\sqrt{6}}\Big)^2\Big(\frac{3}{4}\Big)^d \leqslant m.$$

但如果没有大于 m 个坏的三元集, 我们可以从 $3m$ 个向量中去掉 m 个 $\boldsymbol{x}(i)$ 使得剩下的 $2m$ 个向量不含有坏的三元集, 也就是说, 它们只生成锐角. □

一个大的没有直角的 0/1 点集的 "概率构造" 是很容易实现的, 只要生成随机数后来 "掷钱币". David Bevan 在 $d = 15$ 的情况下构造了一个 31 个点的点集只生成锐角.

附录: 概率论中的三个工具

现在我们介绍离散概率论中三个基本的工具: 随机变量、期望的线性性和 Markov 不等式. 它们将被多次用到.

令 (Ω, p) 为一个有限的概率空间, 也就是说, Ω 是一个有限集, $p = \text{Prob}$ 是一个从 Ω 到区间 $[0,1]$ 且满足 $\sum_{\omega\in\Omega} p(\omega) = 1$ 的映射. Ω 上的一个随机变量 X 是一个映射 $X : \Omega \longrightarrow \mathbb{R}$. 我们在像集上通过令

$$p(X = x) := \sum_{X(\omega)=x} p(\omega)$$

定义一个概率空间 $X(\Omega)$. 一个均匀骰子 (所有的 $p(\omega) = \frac{1}{6}$) 以及 $X =$ "投骰子后在上面的数字" 就是一个简单的例子.

X 的期望 EX 是可能的平均数, 即

$$EX = \sum_{\omega\in\Omega} p(\omega)X(\omega).$$

现在假设 X 和 Y 是两个 Ω 上的随机变量, 那么和 $X + Y$ 也是一个随机变量, 我们有

$$\begin{aligned} E(X+Y) &= \sum_{\omega} p(\omega)(X(\omega) + Y(\omega)) \\ &= \sum_{\omega} p(\omega)X(\omega) + \sum_{\omega} p(\omega)Y(\omega) = EX + EY. \end{aligned}$$

显然, 这可以被推广到有限随机变量的线性组合 —— 这就是所谓的期望的线性性. 注意这不需要随机变量为 "独立" 的假设!

我们的第三个工具涉及只取非负值的随机变量 X, 也就是 $X \geqslant 0$. 令

$$\text{Prob}(X \geqslant a) = \sum_{\omega:X(\omega)\geqslant a} p(\omega)$$

是 X 大于等于正数 a 的概率. 那么

$$EX = \sum_{\omega:X(\omega)\geqslant a} p(\omega)X(\omega) + \sum_{\omega:X(\omega)<a} p(\omega)X(\omega) \geqslant a \sum_{\omega:X(\omega)\geqslant a} p(\omega),$$

我们得到了 *Markov* 不等式

$$\mathrm{Prob}(X \geqslant a) \leqslant \frac{EX}{a}.$$

参考文献

[1] L. Danzer & B. Grünbaum: *Über zwei Probleme bezüglich konvexer Körper von P. Erdős und von V. L. Klee,* Math. Zeitschrift **79** (1962), 95-99.

[2] P. Erdős & Z. Füredi: *The greatest angle among n points in the d-dimensional Euclidean space,* Annals of Discrete Math. **17** (1983), 275-283.

[3] H. Minkowski: *Dichteste gitterförmige Lagerung kongruenter Körper,* Nachrichten Ges. Wiss. Göttingen, Math.-Phys. Klasse 1904, 311-355.

Borsuk 猜想

第 15 章

Karol Borsuk 1933 年发表的论文《关于 n 维 Euclid 球面的三个定理》非常著名, 因为此文中包含一个重要的结果 (由 Stanisław Ulam 所猜测), 即现在熟知的 Borsuk-Ulam 定理:

> 每一个连续映射 $f : S^d \to \mathbb{R}^d$ 都把球面 S^d 的两个对径点映成 $\mathbb{R}^d$ 中的同一点.

Borsuk 的论文非常著名还因为在论文的结尾所提出的一个问题, 即所谓的Borsuk 猜想:

> 具有有限直径 $diam(S) > 0$ 的任一集合 $S \subseteq \mathbb{R}^d$ 是否可以划分成最多 $d+1$ 个直径更小的子集?



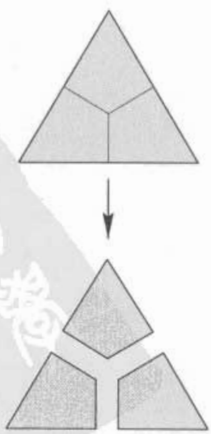
Karol Borsuk

这个界 $d+1$ 是最好的可能: 例如若 S 是一个正则 d 维单纯形, 或者恰为它的 $d+1$ 顶点的集合, 则它的任一使直径变小的划分的每一部分都不能包含多于一个的单纯形顶点. 用 $f(d)$ 表示任一有界集 $S \subseteq \mathbb{R}^d$ 划分成 $f(d)$ 个直径更小的子集的最小值, 则这个正则单纯形的例子表明 $f(d) \geqslant d+1$.

Borsuk 猜想在下列情形下已被证实, 若 S 是一个球面 (由Borsuk 自己所证), S 是光滑体 (利用 Borsuk-Ulam 定理), 或者 $d \leqslant 3, \cdots\cdots$, 但对一般情形此猜想仍未证出. 现在 $f(d)$ 的最好的可用上界是Oded Schramm 给出的, Oded Schramm 证明了对足够大的 d 有

$$f(d) \leqslant (1.23)^d.$$

这个界与猜想 "$f(d) = d+1$" 相比看起来比较弱, 但是当Jeff Kahn 和Gil Kalai 在 1993 年戏剧性地给出了Borsuk 猜想的一个反例, 这个界突然看起来又是有道理的. Borsuk 的论文发表 60 年后, Kahn 和 Kalai 证明了对足够大的 d 有 $f(d) \geqslant (1.2)^{\sqrt{d}}$ 成立.



任一 d- 单纯形可以分裂成 $d+1$ 个部分, 每一部分都具有更小的直径.

后来, A. Nilli 给出的 Kahn-Kalai 证明是一个天书证明: 简短且自完备的, 它在维数 $d = 946$ 时得到了 Borsuk 猜想的一个确切反



A. Nilli

例. 这里我们给出这个证明的一个改进, 是由 Andrei M. Raigorodskii 和 Bernulf Weißbach 给出的, 他们把维数降至 $d = 561$, 更降至 $d = 560$. 现在的 "纪录" 是 $d = 298$, 由 Aicke Hinrichs 和 Christian Richter 在 2002 年所得到.

定理. 设 $q = p^m$ 是一个素数幂, $n := 4q - 2$, 并且$d := \binom{n}{2} = (2q-1)(4q-3)$. 则存在一个集合 $S \subseteq \{+1, -1\}^d$, 它包含了 $\mathbb{R}^d$ 中的 2^{n-2} 个点, 使得 S 的任一每个子部分的直径都更小的划分具有至少

$$\frac{2^{n-2}}{\sum_{i=0}^{q-2}\binom{n-1}{i}}$$

个部分. 当 $q = 9$ 时它推出 Borsuk 猜想在维数 $d = 561$ 时是错误的. 进一步地, 对足够大的 d 有 $f(d) > (1.2)^{\sqrt{d}}$ 成立.

■ **证明.** 集合 S 的构造由下面 4 步进行.

(1) 设 q 是一素数幂, 记 $n = 4q - 2$, 且令

$$Q \ := \ \Big\{\boldsymbol{x} \in \{+1, -1\}^n : x_1 = 1,\ \#\{i : x_i = -1\}\text{为偶数}\Big\},$$

则集合 Q 含有 $\mathbb{R}^n$ 中 2^{n-2} 个向量. 我们将会看到对所有向量 $\boldsymbol{x}, \boldsymbol{y} \in Q$ 有 $\langle \boldsymbol{x}, \boldsymbol{y}\rangle \equiv 2 \pmod 4$ 成立. 我们称 $\boldsymbol{x}, \boldsymbol{y}$ 为近似正交的, 若 $|\langle \boldsymbol{x}, \boldsymbol{y}\rangle| = 2$. 我们将要证明每个不包含近似正交向量的子集 $Q' \subseteq Q$ 一定是 "小的": $|Q'| \leqslant \sum_{i=0}^{q-2}\binom{n-1}{i}$.

(2) 从 Q 出发, 我们构造集合

$$R \ := \ \{\boldsymbol{x}\boldsymbol{x}^T : \boldsymbol{x} \in Q\},$$

它含有 2^{n-2} 个秩为 1 的对称 $(n \times n)$- 矩阵. 我们把它们看成是有 n^2 个分量的向量, 故 $R \subseteq \mathbb{R}^{n^2}$. 我们将证明这些向量之间的夹角都是锐角: 因为它们具有至少为 4 的正内积. 进一步地, 若 $R' \subseteq R$ 不包含内积最小值是 4 的两个向量, 则 $|R'|$ 也是"小的": $|R'| \leqslant \sum_{i=0}^{q-2}\binom{n-1}{i}$.

(3) 从 R 出发, 我们得到一个 $\mathbb{R}^{\binom{n}{2}}$ 中的点的集合:

$$S \ := \ \{(\boldsymbol{x}\boldsymbol{x}^T)_{i>j} : \boldsymbol{x}\boldsymbol{x}^T \in R\},$$

其中点的坐标是相应矩阵的主对角线下方的元素, 同样 S 中有 2^{n-2} 个点. 其中点之间的最大距离恰由那些近似正交的向量 $\boldsymbol{x}, \boldsymbol{y} \in Q$ 所得到. 我们得到比 S 的直径小的子集 $S' \subseteq S$ 一定是 "小的": $|S'| \leqslant \sum_{i=0}^{q-2}\binom{n-1}{i}$.

向量、矩阵和内积

在我们的符号中, 所有的向量 $\boldsymbol{x}, \boldsymbol{y}, \cdots$ 都是列向量; 它们的转置向量 $\boldsymbol{x}^T, \boldsymbol{y}^T, \cdots$ 自然就是行向量了. 矩阵乘积 $\boldsymbol{x}\boldsymbol{x}^T$ 是秩为 1 的矩阵, 这里 $(\boldsymbol{x}\boldsymbol{x}^T)_{ij} = x_i x_j$.

设 $\boldsymbol{x}, \boldsymbol{y}$ 为列向量, 则它们的内积是

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle \;=\; \sum_i x_i y_i \;=\; \boldsymbol{x}^T \boldsymbol{y}.$$

我们也需要两个矩阵 $X, Y \in \mathbb{R}^{n\times n}$ 的内积, 这里我们把矩阵表成长为 n^2 的向量, 从而它们的内积为

$$\langle X, Y \rangle \;:=\; \sum_{i,j} x_{ij} y_{ij}.$$

$$\boldsymbol{x} \;=\; \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \;\Longrightarrow$$

$$\boldsymbol{x}^T = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 \end{pmatrix}$$

$$\boldsymbol{x}\boldsymbol{x}^T = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \end{pmatrix}$$

(4) 估算: 从**(3)** 我们看到对于 S 的每个直径变小的划分都需要至少

$$g(q) \;:=\; \frac{2^{4q-4}}{\sum_{i=0}^{q-2}\binom{4q-3}{i}}$$

个部分. 所以

$$f(d) \;\geqslant\; \max\{g(q), d+1\}, \qquad \text{对于}\;\; d \;=\; (2q-1)(4q-3).$$

从而, 当 $g(q) \;>\; (2q-1)(4q-3)+1$ 时, 我们就得到 Borsuk 猜想在 $d=(2q-1)(4q-3)$ 维空间的一个反例.

下面我们将计算出 $g(9) > 562$, 由此得到在 $d = 561$ 维空间的一个反例. 同时, 我们还有

$$g(q) \;>\; \frac{e}{64\,q^2}\left(\frac{27}{16}\right)^q,$$

它给出了对足够大的 d 来说的一个渐进下界 $f(d) > (1.2)^{\sqrt{d}}$.

(1) 的细节: 我们从一些整除性开始.

引理. *函数 $P(z) := \binom{z-2}{q-2}$ 是一次数为 $q-2$ 的多项式. 对所有整数 z 它都得出整数值. 整数 $P(z)$ 可被 p 整除当且仅当 z 模 q 不同余于 0 或 1.*

断言. 若 $a \equiv b \not\equiv 0 \pmod q$, 则 a 与 b 有相同的 p- 因子个数.

■ **证明.** 记 $a = b + sp^m$, 其中 b 不能被 $p^m = q$ 整除. 所以能整除 b 的任意幂 p^k 满足 $k < m$, 从而 p^k 也能整除 a. 此叙述对 a 和 b 是对称的. □

■ **证明.** 为证明此结论, 我们把这个二项式系数写成

$$P(z) = \binom{z-2}{q-2} = \frac{(z-2)(z-3)\cdot\cdots\cdot(z-q+1)}{(q-2)(q-3)\cdot\ \cdots\ \cdots\ \cdot 2\cdot 1} \qquad (*)$$

并比较其分母和分子的 p- 因子的个数. 因为 $q-1$ 不能被 p 整除, 分母 $(q-2)!$ 所具有的 p- 因子的个数与 $(q-1)!$ 的相同. 的确, 根据边栏处的断言, 如果我们取任意 $q-1$ 个整数, 每一个都取自不同的模 q 非零的剩余类中, 则它们乘积与 $(q-1)!$ 有相同的 p- 因子的个数.

现在若 z 同余于 0 或 $1 \pmod q$, 则分子也是这个样子的: 即乘积中的所有因子都来自于不同的剩余类, 而不会出现的类为含 0 的类 (q 的倍数), 以及包含 -1 或包含 $+1$ 的类, 但是 $+1$ 和 -1 都不能被 p 整除. 所以分母和分子具有相同的 p- 因子个数, 从而商不能被 p 整除.

另一方面, 如果 $z \not\equiv 0, 1 \pmod q$, 则 $(*)$ 的分子中包含一个可被 $q = p^m$ 整除的因子, 同时乘积中没有两个因子来自于相邻的两个非 0 剩余类: 一个代表了没有 p- 因子的数, 而另一个代表的数的 p- 因子个数比 $q = p^m$ 的要少. 所以分子的 p- 因子个数比分母的 p- 因子个数要多, 故商可被 p 整除. □

现在我们考虑不包含近似正交向量的任意子集 $Q' \subseteq Q$, 我们要证实 Q' 一定是 "小的", 也就是 $|Q'| \leqslant \sum_{i=0}^{q-2} \binom{n-1}{i}$.

断言 1. 如果 $\boldsymbol{x}, \boldsymbol{y}$ 是 Q 中不同的向量, 则 $\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2)$ 是一个整数, 所在范围为

$$-(q-2) \leqslant \tfrac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2) \leqslant q-1.$$

因为 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 都具有偶数个 (-1)- 分量, 所以 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 中不同的分量的个数也是偶数. 所以

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle = (4q-2) - 2\#\{i : x_i \neq y_i\} \equiv -2 \pmod 4$$

对所有 $\boldsymbol{x}, \boldsymbol{y} \in Q$ 成立, 即 $\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2)$ 是一个整数.

由 $\boldsymbol{x}, \boldsymbol{y} \in \{+1, -1\}^{4q-2}$ 我们看到 $-(4q-2) \leqslant \langle \boldsymbol{x}, \boldsymbol{y}\rangle \leqslant 4q-2$, 即 $-(q-1) \leqslant \frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2) \leqslant q$. 因为 $x_1 = y_1 = 1$ 推出 $\boldsymbol{x} \neq -\boldsymbol{y}$, 所以下界中的等号是永远不会成立的. 上界中的等号只在 $\boldsymbol{x} = \boldsymbol{y}$ 时成立.

断言 2. 对任意 $\boldsymbol{y} \in Q'$, 由

$$F_{\boldsymbol{y}}(\boldsymbol{x}) := P\big(\tfrac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2)\big) = \binom{\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2) - 2}{q-2}$$

给出的次数为 $q-2$ 的 n 个变元 $x_1,\cdots,x_n$ 的多项式满足对任意 $\boldsymbol{x}\in Q'\backslash\{\boldsymbol{y}\}$, $F_{\boldsymbol{y}}(\boldsymbol{x})$ 可被 p 整除, 但当 $\boldsymbol{x}=\boldsymbol{y}$ 时 $F_{\boldsymbol{y}}(\boldsymbol{x})$ 不能被 p 整除.

这个二项式系数的表达式说明了 $F_{\boldsymbol{y}}(\boldsymbol{x})$ 是一个整数值多项式. 对于 $\boldsymbol{x}=\boldsymbol{y}$, 我们有 $F_{\boldsymbol{y}}(\boldsymbol{y})=1$. 对于 $\boldsymbol{x}\neq\boldsymbol{y}$, 由引理可得到 $F_{\boldsymbol{y}}(\boldsymbol{x})$ 不能被 p 整除当且仅当 $\frac{1}{4}(\langle\boldsymbol{x},\boldsymbol{y}\rangle+2)$ 同余于 0 或 1 $(\bmod q)$. 由断言 1, 这只有当 $\frac{1}{4}(\langle\boldsymbol{x},\boldsymbol{y}\rangle+2)$ 为 0 或 1, 即当 $\langle\boldsymbol{x},\boldsymbol{y}\rangle\in\{-2,+2\}$ 时才能发生. 所以这时 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 一定是近似正交的, 这与 Q' 的定义矛盾.

断言 3. 对 $n-1$ 个变元 $x_2,\cdots,x_n$ 的多项式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ 也有同样的结论, 其中 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ 是如下得到的: 把 $F_{\boldsymbol{y}}(\boldsymbol{x})$ 展开成单项式之和, 通过替换 $x_1=1$, 以及对 $i>1$ 替换 $x_i^2=1$ 去掉变元 x_1, 并且降低所有其他变元的高次幂. 多项式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ 的次数至多为 $q-2$.

所有向量 $\boldsymbol{x}\in Q\subseteq\{+1,-1\}^n$ 都满足 $x_1=1$ 和 $x_i^2=1$. 所以上面的替换并不改变上述多项式在集合 Q 上的取值. 当然这样的替换不可能增加多项式的次数, 所以 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ 的次数至多为 $q-2$.

断言 4. 这些多项式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ 之间没有线性关系 (具有有理系数的), 即多项式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$, $\boldsymbol{y}\in Q'$ 在 $\mathbb{Q}$ 上是线性无关的. 特别地, 它们互不相同.

假设存在形为 $\sum_{\boldsymbol{y}\in Q'}\alpha_{\boldsymbol{y}}\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})=0$ 的一个关系使得系数 $\alpha_{\boldsymbol{y}}$ 不全为 0. 通过乘一个适当的数, 我们可以假设所有的系数都是整数并且不都能被 p 整除. 但是对每个 $\boldsymbol{y}\in Q'$, 取值 $\boldsymbol{x}:=\boldsymbol{y}$ 可得 $\alpha_{\boldsymbol{y}}\overline{F}_{\boldsymbol{y}}(\boldsymbol{y})$ 可被 p 整除, 并且因为 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{y})$ 不能被 p 整除, 我们得到 $\alpha_{\boldsymbol{y}}$ 可被 p 整除.

断言 5. $|Q'|$ 以有 $n-1$ 个变元次数至多为 $q-2$ 且无平方的单项式的个数 $\sum_{i=0}^{q-2}\binom{n-1}{i}$ 为上界.

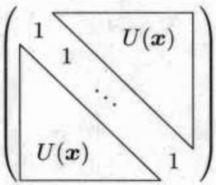
由构造知道多项式 $\overline{F}_{\boldsymbol{y}}$ 是无平方的: 即其中每个单项式中的每个变元的次数都不大于 1. 所以任一 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ 都是 $n-1$ 个变元 $x_2,\cdots,x_n$ 的次数至多为$q-2$ 无平方的单项式的线性组合. 因为这些多项式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ 是线性无关的, 它们的个数 (也就是 $|Q'|$) 不会大于问题中单项式的个数.

(2) 的细节: $\boldsymbol{x}\boldsymbol{x}^T$ 的第 1 列是 $\boldsymbol{x}$, 所以对于不同的 $\boldsymbol{x}\in Q$ 我们得到不同的矩阵 $M(\boldsymbol{x}):=\boldsymbol{x}\boldsymbol{x}^T$. 我们用长为 n^2 的分量为 x_ix_j 的向量来表示这些矩阵. 简单的计算

$$\langle M(\boldsymbol{x}), M(\boldsymbol{y})\rangle \;=\; \sum_{i=1}^{n}\sum_{j=1}^{n}(x_i x_j)(y_i y_j)$$
$$=\; \Big(\sum_{i=1}^{n} x_i y_i\Big)\Big(\sum_{j=1}^{n} x_j y_j\Big) \;=\; \langle \boldsymbol{x},\boldsymbol{y}\rangle^2 \;\geqslant\; 4$$

证明了 $M(\boldsymbol{x})$ 和 $M(\boldsymbol{y})$ 的内积取最小值当且仅当 $\boldsymbol{x},\boldsymbol{y}\in Q$ 是近似正交的.

(3) 的细节: 用 $U(\boldsymbol{x})\in\{+1,-1\}^d$ 表示 $M(\boldsymbol{x})$ 的主对角线下方元素所构成的向量. 因为 $M(\boldsymbol{x})=\boldsymbol{x}\boldsymbol{x}^T$ 是对称的且主对角线上元素都为 $+1$, 我们看到 $M(\boldsymbol{x})\neq M(\boldsymbol{y})$ 可推出 $U(\boldsymbol{x})\neq U(\boldsymbol{y})$. 进一步地,

$M(\boldsymbol{x}) \;=$ 

$$4 \;\leqslant\; \langle M(\boldsymbol{x}), M(\boldsymbol{y})\rangle \;=\; 2\langle U(\boldsymbol{x}), U(\boldsymbol{y})\rangle + n,$$

即

$$\langle U(\boldsymbol{x}), U(\boldsymbol{y})\rangle \;\geqslant\; -\frac{n}{2}+2,$$

等号成立当且仅当 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是近似正交的. 因为所有向量 $U(\boldsymbol{x})\in S$ 具有同样的长度 $\sqrt{\langle U(\boldsymbol{x}), U(\boldsymbol{x})\rangle}=\sqrt{\binom{n}{2}}$, 这意味着点 $U(\boldsymbol{x}), U(\boldsymbol{y})\in S$ 之间的最大距离恰在 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是近似正交时出现.

(4) 的细节: 对于 $q=9$ 我们有 $g(9)\approx 758.31$, 它比 $d+1=\binom{34}{2}+1=562$ 要大.

为得到 d 足够大时的一般的界, 我们应用二项式系数的单调性和单峰性以及估值 $n! > e(\frac{n}{e})^n$ 和 $n! < en(\frac{n}{e})^n$ (参见第 2 章的附录) 可导出

$$\sum_{i=0}^{q-2}\binom{4q-3}{i} < q\binom{4q}{q} = q\,\frac{(4q)!}{q!(3q)!} < q\,\frac{e\,4q\,\left(\frac{4q}{e}\right)^{4q}}{e\left(\frac{q}{e}\right)^{q} e\left(\frac{3q}{e}\right)^{3q}}$$
$$= \frac{4q^2}{e}\Big(\frac{256}{27}\Big)^{q}.$$

从而我们可得到

$$f(d) \;\geqslant\; g(q) \;=\; \frac{2^{4q-4}}{\sum\limits_{i=0}^{q-2}\binom{4q-3}{i}} \;>\; \frac{e}{64q^2}\Big(\frac{27}{16}\Big)^{q}.$$

基于此, 以及

$$d \;=\; (2q-1)(4q-3) \;=\; 5q^2+(q-3)(3q-1) \;\geqslant\; 5q^2, \quad \text{对于} q\geqslant 3,$$

$$q=\tfrac{5}{8}+\sqrt{\tfrac{d}{8}+\tfrac{1}{64}} > \sqrt{\tfrac{d}{8}}, \qquad \text{和} \qquad \big(\tfrac{27}{16}\big)^{\sqrt{\frac{1}{8}}} > 1.2032,$$

我们得到对所有足够大的 d 成立

$$f(d) > \frac{e}{13d}(1.2032)^{\sqrt{d}} > (1.2)^{\sqrt{d}}. \qquad \square$$

注意到当 $q=9$ 时, 商 $g(q) \approx 758$ 比维数 $d(q)=561$ 要大得多, 只取满足 $x_{21}+x_{31}+x_{32}=-1$ 的"四分之三"的 S 中的点即可得到一个维数为 560 的反例.

Borsuk 猜想对 $d \leqslant 3$ 是成立的. 但是对高维情形 Borsuk 猜想并未得到验证. 与之相反的, 如果我们只考虑子集 $S \subseteq \{1,-1\}^d$, 如上面所构造的 (参见 [8]), 直到 $d=8$ 时 Borsuk 猜想都是正确的. 在这两种情形下, 在较低维的空间中找到 Borsuk 猜想的反例都是可能的.

参考文献

[1] K. Borsuk: *Drei Sätze über die n-dimensionale euklidische Sphäre,* Fundamenta Math. **20** (1933), 177-190.

[2] A. Hinrichs & C. Richter: *New sets with large Borsuk numbers,* Preprint, February 2002, 10 pages; Discrete Math., to appear.

[3] J. Kahn & G. Kalai: *A counterexample to Borsuk's conjecture,* Bulletin. Amer. Math. Soc. **29** (1993), 60-62.

[4] A. Nilli: *On Borsuk's problem,* in: "Jerusalem Combinatorics '93" (H. Barcelo and G. Kalai, eds.), Contemporary Mathematics **178**, Amer. Math. Soc. 1994, 209-210.

[5] A. M. Raigorodskii: *On the dimension in Borsuk's problem,* Russian Math. Surveys (6) **52** (1997), 1324-1325.

[6] O. Schramm: *Illuminating sets of constant width,* Mathematika **35** (1988), 180-199.

[7] B. Weissbach: *Sets with large Borsuk number,* Beiträge zur Algebra und Geometrie / Contributions to Algebra and Geometry **41** (2000), 417-423.

[8] G. M. Ziegler: *Coloring Hamming graphs, optimal binary codes, and the 0/1-Borsuk problem in low dimensions,* Lecture Notes in Computer Science **2122**, Springer-Verlag 2001, 164-175.

我们得到对所有足够大的 d 成立

$$f(d) > \frac{c}{13d}(1.2032)^{\sqrt{d}} > (1.2)^{\sqrt{d}}$$ □

注意到当 $q = 9$ 时，而 $g(q) = 758$ 比维数 $d(q) = 561$ 要大得多。只取满足 $x_{21} + x_{31} + x_{32} = -1$ 的"四分之三"的 S 中的点即可得到一个维数为 560 的反例。

Borsuk 猜想对 $d \leq 3$ 是成立的，但是对高维情形 Borsuk 猜想并未得到验证。与之相反的，如果我们只考虑子集 $S \subseteq \{1, -1\}^d$，如上面所构造的 (参见 [8])，直到 $d = 8$ 时 Borsuk 猜想都是正确的。在这两种情形下，在较低维的空间中找到 Borsuk 猜想的反例都是可能的。

参考文献

[1] K. Borsuk: *Drei Sätze über die n-dimensionale euklidische Sphäre*, Fundamenta Math. **20** (1933), 177-190.

[2] A. Hinrichs & C. Richter: *New sets with large Borsuk numbers*, Preprint, February 2002, 10 pages; Discrete Math., to appear.

[3] J. Kahn & G. Kalai: *A counterexample to Borsuk's conjecture*, Bulletin Amer. Math. Soc. **29** (1993), 60-62.

[4] A. Nilli: *On Borsuk's problem*, in: "Jerusalem Combinatorics '93" (H. Barcelo and G. Kalai, eds.), Contemporary Mathematics **178**, Amer. Math. Soc. 1994, 209-210.

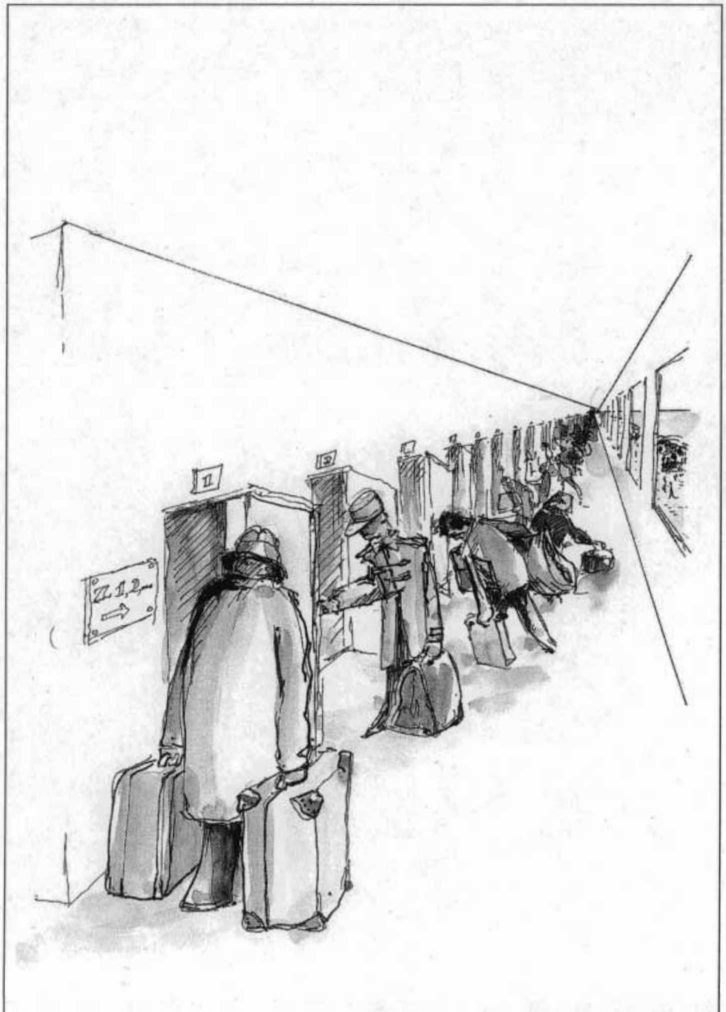
[5] A. M. Raigorodskii: *On the dimension in Borsuk's problem*, Russian Math. Surveys (6) **52** (1997), 1324-1325.

[6] O. Schramm: *Illuminating sets of constant width*, Mathematika **35** (1988), 180-199.

[7] B. Weissbach: *Sets with large Borsuk number*, Beiträge zur Algebra und Geometrie / Contributions to Algebra and Geometry **41** (2000), 417-423.

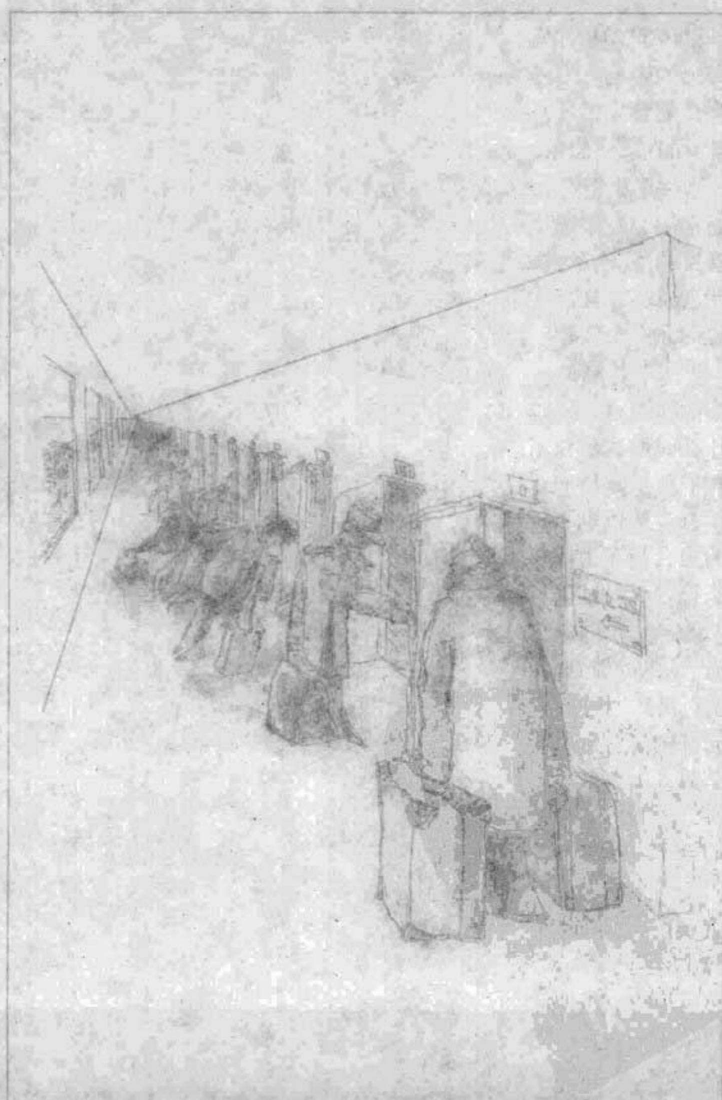
[8] G. M. Ziegler: *Coloring Hamming graphs, optimal binary codes, and the 0/1-Borsuk problem in low dimensions*, Lecture Notes in Computer Science **2122**, Springer-Verlag 2001, 164-175.

分　析



“*Hilbert* 的海滨休闲旅馆”

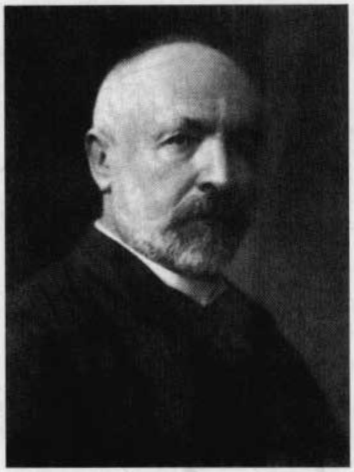
分析



"Hilbert的海滨休闲旅馆"

集合, 函数, 以及连续统假设

第 16 章



Georg Cantor

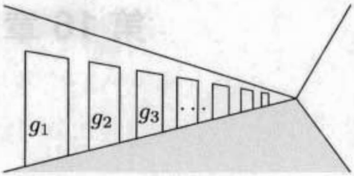
19 世纪后半叶, Georg Cantor 所建立的集合理论对数学产生了深远的影响. 正如 David Hilbert 所说 "没有谁能把我们逐出 Cantor 为我们建立的集合理论这个乐园", 现代数学如果离开了集合的概念, 简直无法想象.

一个集合的 "大小" 或者基是 Cantor 提出的一个基本概念, 我们通常用 $|M|$ 来表示集合 M 的基. 对于有限的集合, 这种表示是显而易见的: 集合的基就是集合所包含的元素个数. 例如 M 包含有 n 个元素, 我们就说 M 是一个 n 元集. 因此 M 和 N 两个集合如果所包含的元素个数相同, 我们就称它们具有相同的基, 即 $|M| = |N|$.

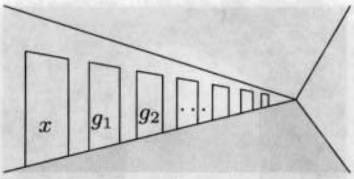
为了将相同基的概念推广到无限集, 我们将运用以下关于有限集的实验给予我们的启发性思想. 假设有一群正要上公交车的人们. 什么时候我们可以说坐车的人数和车上空座位数相等呢? 很简单, 我们只要让所有的人们都坐下, 如果每个人都找到了一个座位, 且没有空座位剩下, 当且仅当这种情况下, 我们可以说由坐车人组成的集合与车上座位组成的集合具有相同的基. 换言之, 两个集合的基相等, 当且仅当在这两个集合之间存在一个双射.

于是我们定义: 任意两个集合 (有限或无限) M 和 N 具有相同的 "大小" 或具有相同的基, 当且仅当在 M 和 N 之间存在一个双射. 显然, 相同基的概念是一个等价关系, 我们可以给每个具有相同基的集合分配一个数, 称之为基数. 例如, 对于有限集合我们得到基数 $0, 1, 2, \cdots, n, \cdots$ 其中 n 代表 n 元集合的类, 特别地, 0 表示空集 $\varnothing$. 通过进一步地观察, 我们得到一个很显然的结论: 有限集合 M 的一个真子集总是比集合 M 小.

当我们考虑无限集合时, 这个理论就变得非常有趣了 (但很不直观). 考虑自然数集合 $\mathbb{N} = \{1, 2, 3, \dots\}$. 如果一个集合 M 可以与 $\mathbb{N}$ 建立一一对应, 我们就称 M 是可数的. 换句话说, 如果我们可以以 $m_1, m_2, m_3, \cdots$ 的形式列出 M 中的元素, 则我们就称 M 是可数的. 但是一种奇怪的现象发生了. 假设我们把一个新元素 x 加入 $\mathbb{N}$, 则 $\mathbb{N} \cup \{x\}$ 仍是可数的, 因此该集合与 N 具有相同的基.



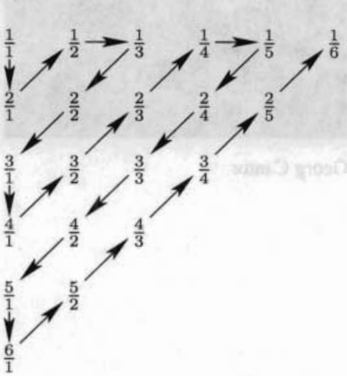
Hilbert 旅馆可以很好地阐述这个事实. 假设一个旅馆有可数个房间, 标记为 $1, 2, 3, \cdots$, 旅客 g_i 住在 i 房间, 所以该旅馆被全部预定了. 现在一个新旅客 x 要求住房, 于是旅店经理告诉他: 对不起, 所有的房间都有人住了. 新来的旅客说, 没问题, 只需要让旅客 g_1 搬到房间 2, 旅客 g_2 搬到房间 3, 旅客 g_3 搬到房间 4, 依此类推, 这样我可以住房间 1. 令旅馆吃惊的是这个方法居然起效了 (因为他不是一个数学家), 他竟可以把所有房客和新房客 x 都安排住宿!



现在旅店老板明白了他同样可以给另外一旅客 y、另一个 z 等等安排住宿. 特别地, 我们知道不同于有限集合, *无限集合 M 存在与其有相同基的真子集*. 事实上, 这是无限集的一个性质即: 一个集合是无限的当且仅当它与自身的某个真子集具有相同的基.

让我们抛开希尔伯特旅馆来看看我们熟悉的由数组成的集合. 整数集 $\mathbb{Z}$ 同样也是可数的, 因为我们可以以 $\{0, 1, -1, 2, -2, 3, -3, \cdots\}$ 的形式来枚举 $\mathbb{Z}$. 更令人吃惊的是我们可以用相似的方式枚举有理数.

定理 1. *有理数集 $\mathbb{Q}$ 是可数集.*



■ **证明.** 按照边图所示将正有理数 $\mathbb{Q}^+$ 列出, 并且删去已经出现的数, 由此我们可知 $\mathbb{Q}^+$ 是可数的. 同理我们将 0 放在 $\mathbb{Q}^+$ 的最前面并且在 $\frac{p}{q}$ 的后边加上 $-\frac{p}{q}$ 得到 $\mathbb{Q}$ 也是可数的. $\mathbb{Q}$ 可以按如下方式列出:

$$\mathbb{Q} = \{0, 1, -1, 2, -2, \tfrac{1}{2}, -\tfrac{1}{2}, \tfrac{1}{3}, -\tfrac{1}{3}, 3, -3, 4, -4, \tfrac{3}{2}, -\tfrac{3}{2}, \cdots\}. \qquad \square$$

以下陈述给出了另一种解释边图的方式:

可数个有限集 M_n 之并仍然是可数的.

事实上, 设集合 $M_n = \{a_{n1}, a_{n2}, a_{n3}, \cdots\}$, 可以如下列出有理数集:

$$\bigcup_{n=1}^{\infty} M_n = \{a_{11}, a_{21}, a_{12}, a_{13}, a_{22}, a_{31}, a_{41}, a_{32}, a_{23}, a_{14}, \cdots\}$$

让我们进一步探讨 Cantor 枚举所有正有理数的方法. 根据边图我们得到以下序列:

$$\tfrac{1}{1}, \tfrac{2}{1}, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{2}{2}, \tfrac{3}{1}, \tfrac{4}{1}, \tfrac{3}{2}, \tfrac{2}{3}, \tfrac{1}{4}, \tfrac{1}{5}, \tfrac{2}{4}, \tfrac{3}{3}, \tfrac{4}{2}, \tfrac{5}{1}, \cdots$$

然后我们得删去重复的数, 例如: $\frac{2}{2} = \frac{1}{1}$ 及 $\frac{2}{4} = \frac{1}{2}$.

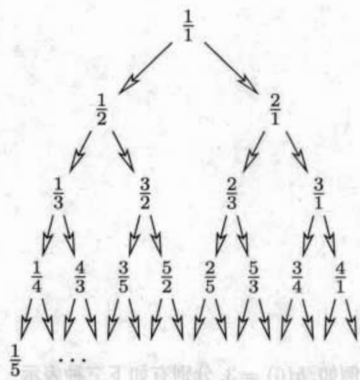
但是, 最近 Neil Calkin 和 Herbert Wilf 发现了一个更优美、更系统的枚举方法, 这个方法保证了枚举过程中不会出现重复的数. 这个新的枚举法按如下方式开始:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, \frac{3}{1}, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}, \frac{5}{2}, \frac{2}{5}, \frac{5}{3}, \frac{3}{4}, \frac{4}{1}, \ldots.$$

这里第 n 个有理数的分母等于第 $(n+1)$ 个数的分子. 换言之, 设 $\left(b(n)\right)_{n\geqslant 0}$ 是如下序列:

$$(1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, \cdots),$$

且第 n 个分数是 $b(n)/b(n+1)$. 德国数学家 Moritz Abraham Stern 在他 1858 年的论文中第一次研究了这个序列, 这个序列也以"Stern 的二价级数"而著称.



我们怎样得到这个序列, 由此得到 Calkin-Wilf 对正分数的枚举呢? 考虑边图中的无穷二权树, 我们不难发现其递归性质:

- $\frac{1}{1}$ 是树根, 且
- 每个结点 $\frac{i}{j}$ 有两个儿子: 左儿子是 $\frac{i}{i+j}$, 右儿子是 $\frac{i+j}{j}$.

我们很容易检验以下四条性质:

(1) 树中所有的分数都是不可约的, 即如果 $\frac{r}{s}$ 出现在树中, 则 r 和 s 是互素的.

树根 $\frac{1}{1}$ 满足上述性质, 然后我们运用归纳法. 如果 r 和 s 是互素的, 则 r 和 $r+s$ 是互素的, s 和 $r+s$ 也是互素的.

(2) 每个在树中出现的不可约分数 $\frac{r}{s} > 0$.

我们对 $r+s$ 运用归纳法. $r+s=2$ 的最小值是 2, 即 $\frac{r}{s}=\frac{1}{1}$, 且这个数出现在树根. 如果 $r>s$, 则 $\frac{r-s}{s}$ 归纳地出现在树中, 于是我们得到 $\frac{r}{s}$ 作为其右儿子. 相似地, 如果 $r<s$, 则 $\frac{r}{s-r}$ 出现在树中, 且 $\frac{r}{s}$ 是其左儿子.

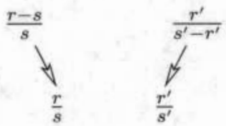
(3) 每个不可约分数在树中只出现一次.

这个证明类似于上述证明. 如果 $\frac{r}{s}$ 出现不只一次, 则 $r \neq s$, 因为树中除了根结点之外其他结点上的数具有形式 $\frac{i}{i+j} < 1$ 或者 $\frac{i+j}{j} > 1$. 但是如果 $r>s$ 或者 $r<s$, 则我们之前已经用归纳法讨论了这些情况.

每个正有理数在树中只出现一次, 因此我们可以一层一层地从左到右地写下这些数. 这样我们就得到了一开始列出的序列.

(4) 在列举的序列中, 第 n 个分数的分母等于第 $(n+1)$ 个数的分子.

当 $n=0$ 或者第 n 个分数是一个左儿子时, 这个性质成立. 设第 n 个数 $\frac{r}{s}$ 是一个右儿子. 如果 $\frac{r}{s}$ 在右边界, 则 $s=1$, 且其后面的数在左边界并且分子为 1. 最后如果 $\frac{r}{s}$ 是内点, 且 $\frac{r'}{s'}$ 是其后面一个分数, 则 $\frac{r}{s}$ 是 $\frac{r-s}{s}$ 的右儿子, $\frac{r'}{s'}$ 是 $\frac{r'}{s'-r'}$ 的左儿子, 且归纳地 $\frac{r-s}{s}$ 的分母是 $\frac{r'}{s'-r'}$ 的分子, 从而我们得到 $s=r'$.



上述结论很漂亮, 但是还有更多精彩的东西. 以下是两个很自然的问题:

- 序列 $(b(n))_{n\geqslant 0}$ 是否有某种特别的 "意义"? 换言之, $b(n)$ 是否等价于一些简单的东西?
- 如果给定 $\frac{r}{s}$, 是否存在一个简单的方法来计算它后面的数?

为了解决第一个问题, 我们计算出结点 $b(n)/b(n+1)$ 的两个儿子分别是 $b(2n+1)/b(2n+2)$ 和 $b(2n+2)/b(2n+3)$. 根据树的结构我们得到如下递归式:

$$b(2n+1)=b(n) \quad 和 \quad b(2n+2)=b(n)+b(n+1). \tag{1}$$

当 $b(0)=1$ 时, 序列 $(b(n))_{n\geqslant 0}$ 由 (1) 完全决定.

是否存在一个 "好的" 或 "已知" 的序列满足上述递归式. 这个问题的答案是肯定的. 我们知道任何一个数 n 可以唯一地表示成 2 的不同幂的和 —— 这就是 n 的二进制表示. n 可以写成 2 的幂之和的形式, 且每个 2^k 至多出现两次, 这种表示法称为 n 的*超二进制*表示. 令 $h(n)$ 是数 n 的超二进制表示的个数. 请读者验证序列 $h(n)$ 满足递归式 (1), 所以对于所有的 n 有 $b(n)=h(n)$ 成立.

例如, $h(6)=3$, 分别有如下三种表示

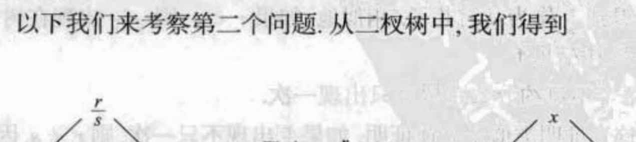
$6=4+2$

$6=4+1+1$

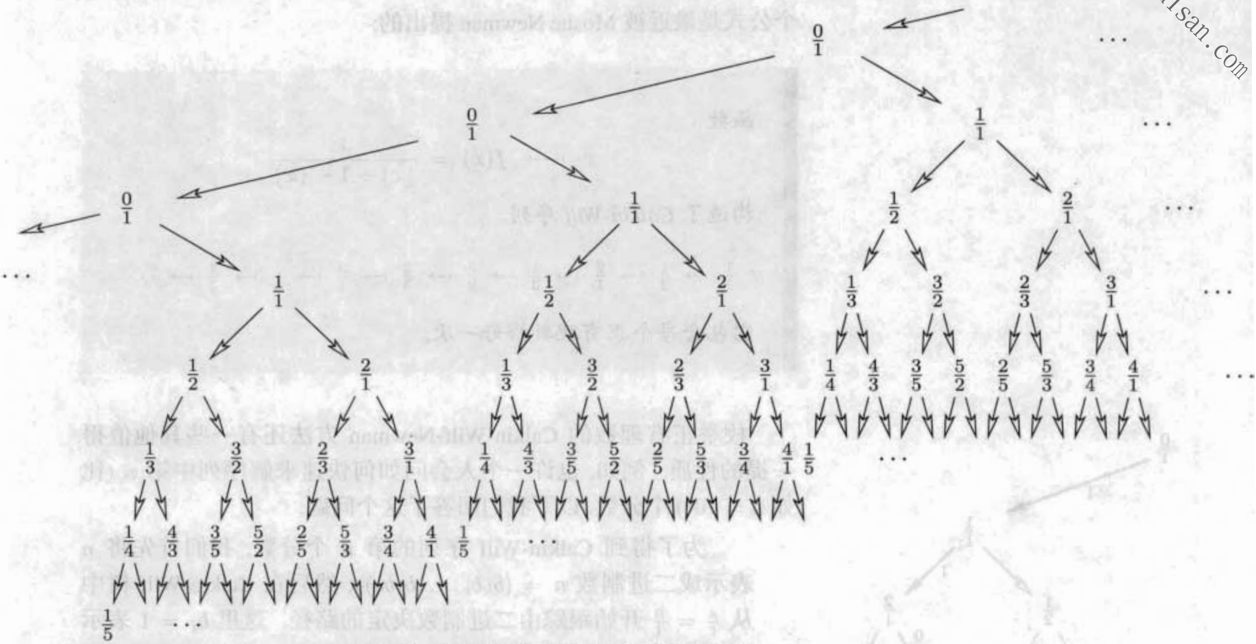
$6=2+2+1+1$.

顺便提一下, 我们已经证明了这样一个事实: 令 $\frac{r}{s}$ 是一个不可约的分数, 则存在一个整数 n 满足 $r=h(n)$ 以及 $s=h(n+1)$.

以下我们来考察第二个问题. 从二权树中, 我们得到

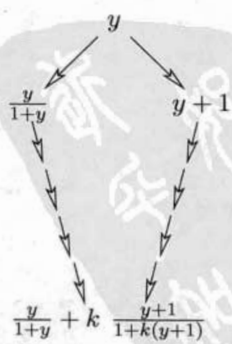


现在我们运用这个来构造一个更大的无限无根二权树, 如下图所示:



在这棵树中, 所有的行是等价的, 它们都表示了所有正有理数的 Calkin-Wilf 枚举 (序列从额外的数 $\frac{0}{1}$ 开始).

怎样从一个有理数得到它后面的数呢? 为了回答这个问题, 对于每个有理数 x, 我们将其右儿子标记为 $x+1$, 右孙子标记为 $x+2$, 依次的我们将第 k 代的右儿子标记为 $x+k$. 相似地, x 的左儿子是 $\frac{x}{1+x}$, $\frac{x}{1+x}$ 的左儿子是 $\frac{x}{1+2x}$, 依次地, x 的第 k 代的左儿子是 $\frac{x}{1+kx}$.



现在为了从 $\frac{r}{s}=x$ 得到序列的下一个有理数 $f(x)$, 我们来分析一下边图所示的情形. 事实上, 我们考虑无穷二权树中的任何非负有理数 x, 它是某个有理数 $y \geqslant 0$ 的左儿子的第 $k(k \geqslant 0)$ 代的右儿子, 同时 $f(x)$ 是同一个 y 的右儿子的第 k 代的左儿子. 因此根据第 k 代左右儿子的公式, 我们得到边图中所要阐述的等式:

$$x = \frac{y}{1+y}+k,$$

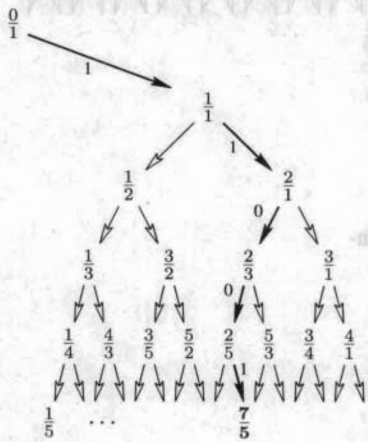
这里我们用 $k=\lfloor x\rfloor$ 表示 x 的整数部分, $\frac{y}{1+y}=\{x\}$ 表示其小数部分. 由此我们得到:

$$f(x)=\frac{y+1}{1+k(y+1)}=\frac{1}{\frac{1}{y+1}+k}=\frac{1}{k+1-\frac{y}{y+1}}=\frac{1}{\lfloor x\rfloor+1-\{x\}}.$$

因此我们得到由有理数 x 求其后继有理数 $f(x)$ 的一个漂亮公式, 这

个公式是最近被 Moshe Newman 提出的:

> 函数
> $$x \longmapsto f(x) = \frac{1}{\lfloor x \rfloor + 1 - \{x\}}$$
> 构造了 *Calkin-Wilf* 序列
> $$\tfrac{1}{1} \mapsto \tfrac{1}{2} \mapsto \tfrac{2}{1} \mapsto \tfrac{1}{3} \mapsto \tfrac{3}{2} \mapsto \tfrac{2}{3} \mapsto \tfrac{3}{1} \mapsto \tfrac{1}{4} \mapsto \tfrac{4}{3} \mapsto \cdots$$
> 它包含每个正有理数恰好一次.



枚举正有理数的 Calkin-Wilf-Newman 方法还有一些其他值得一提的性质. 例如, 也许一个人会问如何快速求解序列中第 n (比如 $n = 10^6$) 个分数. 以下我们回答了这个问题:

为了得到 Calkin-Wilf 序列的第 n 个分数, 我们首先将 n 表示成二进制数 $n = (b_k b_{k-1} ... b_1 b_0)_2$, 然后在 Calkin-Wilf 树中从 $\frac{s}{t} = \frac{0}{1}$ 开始跟踪由二进制数决定的路径. 这里 $b_i = 1$ 表示 "选择右儿子", 即 "将分母加到分子上"; 而 $b_i = 0$ 表示 "选择左儿子", 即 "将分子加到分母上."

边图展示了由 $n = 25 = (11001)_2$ 决定的路径: 因此 Calkin-Wilf 序列中的第 25 个数是 $\frac{7}{5}$. 读者可以很容易地找到一个类似的方法来确定一个给定分数 $\frac{s}{t}$(二进制表示) 在 Calkin-Wilf 序列中的位置 n.

现在我们来考虑实数 $\mathbb{R}$. 它们也是可数的吗? 它们是不可数, 并且证明这个性质的 Cartor 对角线方法, 不仅是所有集合论的重要基础, 而且这个绝妙的证明是出自于数学天书.

定理 2. 实数全体 $\mathbb{R}$ 是不可数的.

■ **证明.** 任何一个可数集 $M = \{m_1, m_2, m_3, \cdots\}$ 的子集 N 是至多可数的 (即有限或可数). 事实上, 只要按 M 中同样的方法列举 N 即可. 因此, 如果我们可以找到 $\mathbb{R}$ 的一个不可数的子集, 则就证明了 $\mathbb{R}$ 是不可数的. 我们考察 $\mathbb{R}$ 的子集 $M = (0, 1]$, 即所有 $0 < r \leqslant 1$ 的正实数 r. 假设 M 可数, 则 M 可列, 令 $M = \{r_1, r_2, r_3, \cdots\}$. 我们将 r_n 记成末尾没有无穷个 0 的无穷十进制表示, 且这种表示方法是唯一的:

$$r_n = 0.a_{n1} a_{n2} a_{n3} ...$$

其中对于所有 n 和 i 有 $a_{ni} \in \{0, 1, \cdots, 9\}$. 例如, $0.7 = 0.6999 \cdots$.

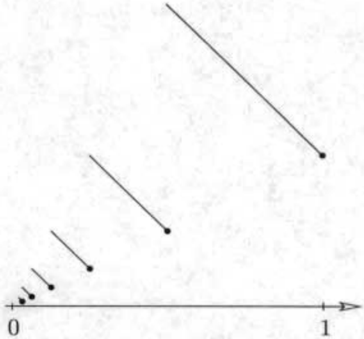
考虑如下二维无限数组:

$$\begin{array}{rcl} r_1 & = & 0.a_{11}a_{12}a_{13}\ldots \\ r_2 & = & 0.a_{21}a_{22}a_{23}\ldots \\ \vdots & & \vdots \\ r_n & = & 0.a_{n1}a_{n2}a_{n3}\ldots \\ \vdots & & \vdots \end{array}$$

对每个 n, 我们选择 $b_n \in \{1, \cdots, 8\}$ 且 b_n 不同于 a_{nn}; 这显然是可以办到的. 那么 $b = 0.b_1b_2b_3\ldots b_n\ldots$ 是集合 M 中的一个实数, 所以 b 有一个标号, 比如 $b = r_k$. 但是由于 b_k 是不同于 a_{kk} 的, 所以 b_k 的标号不是 r_k, 这就产生了矛盾. 这就是定理的证明! □

我们多观察一下实数, 则发现 $(0,1), (0,1], [0,1)$ 和 $[0,1]$ 区间具有相同的基. 例如, 我们将证明 $(0,1]$ 和 $(0,1)$ 具有相同的基, 如下定义的映射可以证明这个结论 $f: (0,1] \longrightarrow (0,1), x \longmapsto y$:

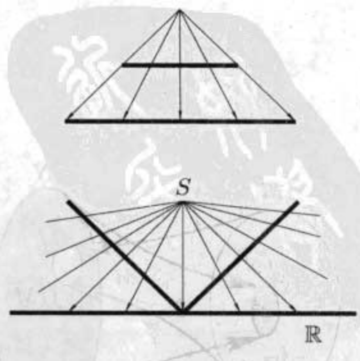
$$y := \begin{cases} \frac{3}{2} - x & \text{当} \quad \frac{1}{2} < x \leqslant 1, \\ \frac{3}{4} - x & \text{当} \quad \frac{1}{4} < x \leqslant \frac{1}{2}, \\ \frac{3}{8} - x & \text{当} \quad \frac{1}{8} < x \leqslant \frac{1}{4}, \\ \vdots & \end{cases}$$



一个双射 $f: (0,1] \longrightarrow (0,1)$

由于在第一条线上 y 的范围是 $\frac{1}{2} \leqslant y < 1$, 在第二条线上是 $\frac{1}{4} \leqslant y < \frac{1}{2}$, 在第三条线上是 $\frac{1}{8} \leqslant y < \frac{1}{4}$, 依次类推, 我们可以知道映射 f 是双射.

通过考虑边图的中心映射, 我们知道任何两个区间 (区间长度大于零且有限) 具有相同的基. 更进一步: 任何长度大于 0 的区间和实数轴 $\mathbb{R}$ 具有相同的基. 为了证明这个, 我们考虑弯曲的 $(0,1)$ 区间, 以 S 为中心将其映满 $\mathbb{R}$.



因此, 我们得到如下结论: 任何长度大于 0 的开区间, 半开半闭区间, 闭区间 (有限或无限) 具有相同的基, 并记此基为 c, 这个 c 表示连续统 ($[0,1]$ 区间有时也被称作连续统).

经过仔细思考, 我们也许能够得到有限和无限区间具有相同基的结论, 但是下面的结论明显是有背于我们的直觉.

定理 3. 由 $\mathbb{R}$ 的所有有序实数对构成的集合 $\mathbb{R}^2$ (即实平面) 与 $\mathbb{R}$ 具有相同的基.

■ **证明.** 我们只需证明任何有序实数对 (x, y), $0 < x, y \leqslant 1$ 可以和 $(0, 1]$ 区间建立双射. 这个证明仍然源于数学天书. 考虑任一有序数对 (x, y), 并且将其写成如下无终结的唯一十进制展开形式. 例如:

$$\begin{aligned} x &= 0.3 \quad 01 \quad 2 \quad 007 \quad 08 \quad \cdots \\ y &= 0.009 \quad 2 \quad 05 \quad 1 \quad 0008 \quad \cdots \end{aligned}$$

按上述方法, 我们通过找下一个不为零的数字可以将 x 和 y 的十进制形式分成一系列组. 现在我们先写下 x 的第一组, 再写下 y 的第一组, 然后写下 x 的第二组, 依次类推, 我们将 (x, y) 合并成 $z \in (0, 1]$. 因此, 就上述的例子, 我们得到如下实数:

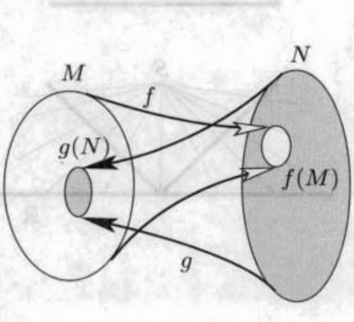
$$z = 0.3\,009\,01\,2\,2\,05\,007\,1\,08\,0008 \cdots$$

因为 x 和 y 都是无限十进制小数, 所以通过如上方法得到的 z 也是无限十进制小数. 相反地, 从 z 的无限十进制展开形式, 我们也可以得到 (x, y), 故这个映射是双射, 故定理得证. □

由于 $(x, y) \longmapsto x + iy$ 是 $\mathbb{R}^2$ 到复数 $\mathbb{C}$ 的双射, 我们得到结论: $|\mathbb{C}| = |\mathbb{R}| = c$. 为什么 $|\mathbb{R}^2| = |\mathbb{R}|$ 这样出乎意料呢? 这是因为这个事实有背于我们关于维数的直观理解. 它表明了 2 维平面 $\mathbb{R}^2$ (归纳地, 一般的 n 维空间 $\mathbb{R}^n$) 可以同 1 维实数轴 $\mathbb{R}$ 建立双射. 因此维数不是双射下的不变量. 但是如果我们要求一个映射和这个映射的逆都是连续的, 这种情况下维数是不变的, 这个事实是由 Luitzen Brouwer 最先证明的.

让我们进一步地深入思索. 到目前为止, 我们有了相同基的概念. 什么时候我们会说 M 至多和 N 一样大呢? 同样, 映射是解决这个问题的关键. 设 $|M| = \mathbf{m}$, $|N| = \mathbf{n}$, 如果存在一个从 M 到 N 的单射, 我们就说基数 $\mathbf{m}$ 不大于 $\mathbf{n}$. 显然, $\mathbf{m} \leqslant \mathbf{n}$ 是不依赖于代表集合 M 和 N 的选取的. 对于有限集合, 这个概念与我们的直观理解是一致的: 一个 m 元集合至多和一个 n 元集合一样大当且仅当 $m \leqslant n$.

现在我们面临一个基本的问题. 我们知道有关不等式的一般准则对于有限基数是成立的, 但是对于无限基数是否成立呢? 特别地, 如果 $\mathbf{m} \leqslant \mathbf{n}$, $\mathbf{n} \leqslant \mathbf{m}$ 是否有 $\mathbf{m} = \mathbf{n}$? 这个结论并非显而易见的: 给定无限集合 M, N 以及单射 $f : M \longrightarrow N$ 和单射 $g : N \longrightarrow M$, 它们不需要是满射. 我们得到启发, 也许可以根据以上两个单射构建一个从 M 到 N 的双射. 但是, 我们并不清楚具体的对应关系.



1883 年 Cantor 宣布的著名的 Schröder-Bernstein 定理解决了上述问题. 这个定理首先是被 Friedrich Schröder 证明的, Felix Bernstein 在一段时间之后也证明了该定理. 接下来的证明出现在 20 世纪集

合论天才 Paul Cohen 的一本小册子中, Paul Cohen 因解决了连续统假设问题而闻名于世 (在以后的章节中我们会来讨论这个问题).

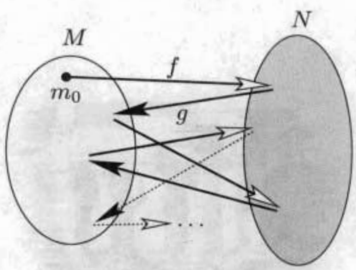


"Schröder 和 Bernstein 在画画"

定理 4. 如果两个集合 M 和 N 之间可以建立到对方内的单射, 那么在 M 和 N 之间存在一个双射, 即 $|M| = |N|$.

■**证明.** 我们首先假设 M 和 N 不相交 —— 如果不是, 我们可以用一个新的集合去替代 N.

f 将 M 中的元素映到 N, g 将 N 中的元素映到 M. 一种将这个混乱的局面变清晰和有序的方法就是将 $M \cup N$ 的元素排列成许多链: 从 M 中任选一个元素 $m_0 \in M$, 然后将 f 作用在 m 上, 再将 g 作用在 $f(m)$ 上, 依次类推我们可以得到一条链. 如果 m_0 再次出现在链中, 那么这条链就是封闭的 (情形 1); 也有可能这条链是无限的且每个元素不相等. (由于 f 和 g 是单射的, 我们知道链中第一个出现的重复元素一定是 m_0)



如果一条链无限重复下去, 我们试图向后跟踪它: 如果 m_0 是 g 的像, 则将 m_0 连接到 $g^{-1}(m_0)$, 然后, 如果 $g^{-1}(m_0)$ 是 f 的像, 则将 $g^{-1}(m_0)$ 连接到 $f^{-1}(g^{-1}(m_0))$, 依次类推. 这样会出现其他三种情况: 向后跟踪这条链也许会无限进行下去 (情形 2), 也可能在一个不是映射 g 的像 M 的元素处停下来 (情形 3), 也有可能在一个不是映射 f 的像 N 的元素处停下来 (情形 4).

因此 $M \cup N$ 被划分成四种互不相交的链, 这些链中的元素可以以某种方式标记, 使得我们可以证明 $F : m_i \longmapsto n_i$ 是双射. 我们就以上四种情形分别地讨论:

情形 1. $2k+2$ 个不同元素的有限圈 ($k \geqslant 0$)

$$m_0 \xrightarrow{f} n_0 \xrightarrow{g} m_1 \xrightarrow{f} \cdots \quad m_k \xrightarrow{f} n_k \xrightarrow{g} m_0$$

情形 2. 双向无限链, 且链中每个元素不同

$$\cdots \longrightarrow m_0 \xrightarrow{f} n_0 \xrightarrow{g} m_1 \xrightarrow{f} n_1 \xrightarrow{g} m_2 \xrightarrow{f} \cdots$$

情形 3. 始于元素 $m_0 \in M\backslash g(N)$ 的单向无限链, 且链中每个元素不同

$$m_0 \xrightarrow{f} n_0 \xrightarrow{g} m_1 \xrightarrow{f} n_1 \xrightarrow{g} m_2 \xrightarrow{f} \cdots$$

情形 4. 始于元素 $n_0 \in N\backslash f(M)$ 的单向无限链, 且链中每个元素不同

$$n_0 \xrightarrow{g} m_0 \xrightarrow{f} n_1 \xrightarrow{g} m_1 \xrightarrow{f} \cdots$$

□

关于不等式问题的其他关系式呢? 一般来讲, 如果 $\mathfrak{m} \leqslant \mathfrak{n}$ 且 $\mathfrak{m} \neq \mathfrak{n}$, 则我们规定 $\mathfrak{m} < \mathfrak{n}$. 我们知道任意两个基数 $\mathfrak{m}$ 和 $\mathfrak{n}$ 以下三种情形至多有一个成立:

$$\mathfrak{m} < \mathfrak{n},\ \mathfrak{m} = \mathfrak{n},\ \mathfrak{m} > \mathfrak{n}$$

事实上, 基数定理指出以上三种情形有且仅有一种成立. (参见本章附录中命题 2.)

进一步, Schröder-Bernstein 定理还告诉我们关系 $<$ 是可传递的, 即由 $\mathfrak{m} < \mathfrak{n}$ 和 $\mathfrak{n} < \mathfrak{p}$ 我们可以得到 $\mathfrak{m} < \mathfrak{p}$. 因此, 基数可以排成一个始于有限基 $0, 1, 2, 3, \cdots$ 的线性序列. 根据 Zermelo-Fraenkel 公理系统 (特别地, 选择公理), 我们可以容易知道任何无限集 M 包含一个可数的子集. 事实上, M 包含一个元素, 设为 m_1. 集合 $M\backslash\{m_1\}$ 非空 (因为 M 是无限的), 故其含有元素 m_2. 考虑集合 $M \setminus \{m_1, m_2\}$, 我们可以知道 m_3 的存在性, 依次类推. 所以, 可数集的基是最小的无限基, 通常我们用 $\aleph_0$ 表示, 读作 "aleph zero".



"最小的无限基数"

作为对于任意无限基 $\mathfrak{m}$ 有 $\aleph_0 \leqslant \mathfrak{m}$ 的一个推论, 我们可以很快证明对于任意无限基 $\mathfrak{m}$ 的 "希尔伯特旅店" 问题, 即, 对于任何无限集合 M, 有 $|M \cup \{x\}| = |M|$. 事实上, M 包含子集 $N = \{m_1, m_2, m_3, \cdots\}$. 现在我们将 x 映到 m_1, m_1 映到 m_2, 依次类推, 且 $M\backslash N$ 中的元素映到自身. 这样就给出了 M 和 $M \cup \{x\}$ 之间的双射.

由此我们也证明了一个早先提到的结果: 每个无限集都与一些真子集有相同的基数.

作为 Schröder-Bernstein 定理的另外一个结果我们可以证明 $\mathbb{N}$

的所有子集构成的集合 $\mathcal{P}(\mathbb{N})$ 的基数是 c. 要证明这个结论, 我们只需证明 $|\mathcal{P}(\mathbb{N})\backslash\{\varnothing\}| = |(0,1]|$. 以下例子建立了一个单射:

$$f:\mathcal{P}(\mathbb{N})\setminus\{\varnothing\} \longrightarrow (0,1], \qquad A \longmapsto \sum_{i\in A}10^{-i},$$

同时

$$g:(0,1] \longrightarrow \mathcal{P}(\mathbb{N})\setminus\{\varnothing\}, \qquad 0.b_1b_2b_3... \longmapsto \{b_i 10^i : i\in\mathbb{N}\}$$

定义了另一个方向上的单射.

到目前为止, 我们知道基数 $0,1,2,\cdots,\aleph_0$, 且 $\mathbb{R}$ 的基数 c 大于 $\aleph_0$. 从 $\mathbb{Q}$ 的基 $|\mathbb{Q}|=\aleph_0$ 到 $\mathbb{R}$ 的基 $|\mathbb{R}|=c$ 之间的空缺引出了如下问题:

$c=|\mathbb{R}|$ 是否是紧接 $\aleph_0$ 后的无限基?

当然, 现在我们面临着一个问题: 是否存在一个更大的基数, 或者 $\aleph_1$ 是否有意义. 它的确有意义 —— 在本章的附录中我们有一个简要证明.

$c=\aleph_1$ 就是著名的*连续统假设定理*. 许多年以前, 连续统假设是最具挑战的数学难题之一. 最后由 Kurt Gödel 和 Paul Cohen 给出的答案让我们触碰到逻辑思想的极限. 他们证明 $c=\aleph_1$ 是不依赖于 Zermelo-Fraenkel 公理系统的, 就像平行公理是不依赖其他欧几里得几何公理一样. 在集合论中既存在 $c=\aleph_1$ 的模型, 也存在 $c\neq\aleph_1$ 的模型.

鉴于这个事实, 一个有意思的问题是: 是否存在其他等价于连续统假设的情形 (比如从分析上考虑) . 事际上, 寻求一个分析上的例子是很自然的想法, 因为历史上 Cartor 集合论的第一个重要的应用就是出现在分析中, 特别是复变函数理论. 以下我们将给出一个例子, 这个例子优美且简洁的解是由 Paul Erdős 给出的. 1962 年, Wetzel 提出了如下问题:

> *令 $\{f_\alpha\}$ 是复数域上两两不同的解析函数族, 且满足对于任何 $z\in\mathbb{C}$ 集合 $\{f_\alpha(z)\}$ 至多可数 (即, 要么有限要么可数); 我们把这个性质称作 (P_0).*
>
> *是否函数族自身至多是可数的呢?*

出人意料地, Erdős 很快地证明了这个是依赖于连续统假设的.

定理 5. 如果 $c > \aleph_1$, 则对于任意满足 (P_0) 的函数族 $\{f_\alpha\}$ 是可数的. 另一方面, 如果 $c = \aleph_1$, 则存在满足性质 (P_0) 且基为 c 的函数族 $\{f_\alpha\}$.

为了证明这个结论, 我们需要关于基数和序数的一些基本事实. 对于不太熟悉这部分内容的读者可以参见本章附录, 其中列出了所有必要的结果.

■ **定理 5 的证明.** 假设 $c > \aleph_1$. 我们要证明对于任意基数为 $\aleph_1$ 的解析函数族 $\{f_\alpha\}$, 存在一个复数 z_0 使得所有 $\aleph_1$ 个 $f_\alpha(z_0)$ 的函数值是不同的. 因此, 如果一个函数族满足 (P_0), 则它是可数的.

为了证明这个, 我们将运用有关序数的知识. 首先我们根据 $\aleph_1$ 的初始序数 ω_1 将函数族 $\{f_\alpha\}$ 良序化. 根据附录中的命题 1 我们知道这个指标集包含了所有比 ω_1 小的序数 α. 接下来我们要证明由满足 $\alpha < \beta < \omega_1$ 的点对 (α, β) 构成的集合的基是 $\aleph_1$. 因为任意 $\beta < \omega_1$ 是一个可数的序数, 故对于每个固定的 β, 由点对 (α, β), $\alpha < \beta$ 构成的集合是可数的. 对 $\aleph_1$ 个 β 求并, 根据附录中的命题 6 我们知道由点对 (α, β), $\alpha < \beta$ 构成的集合基是 $\aleph_1$.

对于 $\alpha < \beta$, 考虑如下集合:

$$S(\alpha, \beta) = \{z \in \mathbb{C} : f_\alpha(z) = f_\beta(z)\}.$$

我们要证集合 $S(\alpha, \beta)$ 是可数的. 为了证明这个结论, 我们考虑复平面上以原点为圆心, 以 $k = 1, 2, 3, \cdots$ 为半径的圆 C_k. 如果 f_α 和 f_β 在 C_k 中有无限个点相等, 则由著名的解析函数定理我们知道 f_α 和 f_β 是恒等的. 因此, f_α 和 f_β 只在每个 C_k 中有限个元素上相等, 从而它们只在至多可数个点上函数值相等. 我们令 $S := \bigcup_{\alpha<\beta} S(\alpha, \beta)$. 由于每个集 $S(\alpha, \beta)$ 是可数的, 同样由命题 6, 我们知道 S 与 $\aleph_1$ 具有相同的基. 从而我们得到结论: 这是因为 $\mathbb{C}$ 的基是 c, 且由假设知 c 比 $\aleph_1$ 更大, 故存在一个不属于 S 的复数 z_0 使得每个 $f_\alpha(z_0)$ 的值都是不相同的.

接下来我们假设 $c = \aleph_1$. 考虑实部和虚部都为有理数的复数 $p + iq$ 构成的集合 $D \subseteq \mathbb{C}$. 由于对每个 p 集合 $\{p + iq : q \in \mathbb{Q}\}$ 是可数的, 则 D 是可数的. 进一步地, D 是 $\mathbb{C}$ 中的稠密集: 复平面中的任何开区域包含 D 中的点. 令 $\{z_\alpha : 0 \leqslant \alpha < \omega_1\}$ 是 $\mathbb{C}$ 的一个良序排列. 现在我们要构造 $\aleph_1$ 个不同的解析函数构成的函数族 $\{f_\beta : 0 \leqslant \beta < \omega_1\}$ 使得下式成立

$$当\ \alpha < \beta\ 时\quad f_\beta(z_\alpha) \in D. \tag{1}$$

任何这样的函数族满足条件 (P_0). 实际上, $\mathbb{C}$ 中的每个点 $z \in \mathbb{C}$ 对应于一个指标, 设为 $z = z_\alpha$. 现在, 对于任何 $\beta > \alpha$, $\{f_\beta(z_\alpha)\}$ 的函数值存在于可数集 D 中. 因为 α 是可数序数, 对于满足 $\beta \leqslant \alpha$ 的 f_β 至多只有可数个 $\{f_\beta(z_\alpha)\}$. 同样, 所有函数值的集合 $\{f_\beta(z_\alpha)\}$ 也至多是可数的. 因此如果我们能构造出满足 (1) 的函数族 $\{f_\beta\}$, 则定理的第二部分就得证了.

我们通过超限递归法来构造 $\{f_\beta\}$. 我们可以选择任意解析函数作为 f_0, 比如令其为常数函数. 假设对于 $\beta < \gamma$ 我们已经构造出 f_β. 因为 γ 是一个可数序数, 我们可以将 $\{f_\beta : 0 \leqslant \beta < \gamma\}$ 记成一个序列 $g_1, g_2, g_3, \cdots$. $\{z_\alpha : 0 \leqslant \alpha < \gamma\}$ 的同样排列也可以得到一个序列 $w_1, w_2, w_3, \cdots$. 对于每个 n, 我们现在可以构造满足如下条件的 f_γ:

$$f_\gamma(w_n) \in D \quad 且 \quad f_\gamma(w_n) \neq g_n(w_n). \tag{2}$$

第二个条件保证了所有函数 f_γ $(0 \leqslant \gamma < \omega_1)$ 是不同的, 且仅第一个条件就可以推出 (P_0). 注意到条件 $f_\gamma(w_n) \neq g_n(w_n)$ 又是一次对角化论证.

为了构造 f_γ, 我们记下

$$\begin{aligned} f_\gamma(z) \;:=\; & \varepsilon_0 + \varepsilon_1(z - w_1) + \varepsilon_2(z - w_1)(z - w_2) \\ & + \varepsilon_3(z - w_1)(z - w_2)(z - w_3) + \cdots . \end{aligned}$$

如果 γ 是有限序数, 则 f_γ 是一个多项式, 故其是解析的, 且我们可以找到数 ε_i 使其满足条件 (2). 现在我们考虑 γ 是可数序数的情形, 则

$$f_\gamma(z) \;=\; \sum_{n=0}^{\infty} \varepsilon_n (z - w_1) \cdots (z - w_n). \tag{3}$$

注意到 ε_m $(m \geqslant n)$ 的值对 $f_\gamma(w_n)$ 的值没有影响, 因此我们可以一步一步地选择 ε_n. 如果序列 (ε_n) 很快地收敛到 0, 则 (3) 定义了一个解析函数. 最后, 因为 D 是稠密集, 我们可以选择这样的序列 (ε_n) 使得 f_γ 满足要求 (2), 这样我们就完成了定理 5 的证明. □



"这幅图画讲述了 *St. Augustin* 沿着海滨踱步沉思无穷问题时, 看到一个小孩试图用一个小贝壳把海水舀空的故事..."

附录: 基数与序数

首先我们来考虑对于每个基数是否存在紧接其后的另一个更大基数的问题. 我们先证明对每个基数 $\mathbf{m}$, 都存在比其大的基数 $\mathbf{n}$. 我们同样用 Cantor 对角化法则来证明这个问题.

设 M 是一个集合, 则由 M 所有子集构成的集合 $\mathcal{P}(M)$ 比 M 大. 将 $m \in M$ 对应 $\{m\} \in \mathcal{P}(M)$, 我们知道 M 可以和 $\mathcal{P}(M)$ 的子集建立双射, 根据定义有$|M| \leqslant |\mathcal{P}(M)|$. 我们还得证明 $\mathcal{P}(M)$ 不能和 M 的子集建立双射. 否则, 设 $\varphi : N \longrightarrow \mathcal{P}(M)$ 是从 $N \subseteq M$ 到 $\mathcal{P}(M)$ 的双射. 考虑 N 中满足如下性质的子集 U: 任何 U 中的元素不包含于其在映射 φ 的像里, 即 $U = \{m \in N : m \notin \varphi(m)\}$. 因为 φ 是双射, 故存在 $u \in N$ 使得 $\varphi(u) = U$. 现在, 要么有 $u \in U$ 要么 $u \notin U$, 但是两种情况都是不可能发生的. 事实上, 如果 $u \in U$, 则由 U 的定义我们知道 $u \notin \varphi(u) = U$; 另一方面如果 $u \notin U = \varphi(u)$, 则 $u \in U$, 从而产生矛盾.

读者很可能看过这样的证明. 有一个古老的关于理发师的难题讲的就是这样的问题: "如果一个理发师帮助所有不给自己剃胡子的人剃胡子, 那么这个理发师会给自己剃胡子吗?"

为了得到更进一步的理论, 我们引进 Cantor 提出的又一伟大的概念, 序集和序数. 如果 $<$ 关系在集合 M 中有传递性, 且对于 M 中任意两个不同的数 a 和 b 要么 $a < b$ 要么 $b < a$, 则 M 可以根据 $<$ 关系排序. 例如, 我们可以根据数量关系将 $\mathbb{N}$ 排序, 即 $\mathbb{N} = \{1, 2, 3, 4, \cdots\}$, 但是我们还可以从反方向将 $\mathbb{N}$ 排序即 $\mathbb{N} = \{\cdots, 4, 3, 2, 1\}$, 或者我们也可以通过先列出奇数再列出偶数得到另一种排序方法, $\mathbb{N} = \{1, 3, 5, \cdots, 2, 4, 6, \cdots\}$.

这里有一个重要的概念. 如果一个序集的每个非空子集有第一个元素, 则称该集合是*良序的*. 因此上述 $\mathbb{N}$ 的第一种和第三种排列都是良序的, 而第二种排列不是. 基本的*良序定理*是从公理 (包括选择公理) 得到的, 它说的是: *任何一个集合都存在一个良序排列*. 从现在开始我们考虑的集合都是赋予了一个良序的集合.

良序集 $\mathbb{N} = \{1, 2, 3, \cdots\}$ 和 $\mathbb{N} = \{1, 3, 5, \cdots, 2, 4, 6, \cdots\}$ 不是相似的: 第一种排列中只存在一个没有前导的元素, 而第二种排列中存在两个这样的元素.

如果在两个良序集 M 和 N 之间存在保持序关系的双射 φ, 即, 从 $m <_M n$ 可以推出 $\varphi(m) <_N \varphi(n)$, 则称 M 和 N 是*相似的* (或具有相同序型). 显然地, 任何同一个良序集相似的序集其本身也是良序的.

相似性是一种等价关系, 因此*序数* α 是属于一类相似集的. 对于有限集, 任何两种排列都是相似良序排列, 且我们用序数 n 来表示 n 元集. 根据定义, 我们知道两个相似集是具有相同基数的. 因此, 序数 α 的*基数* $|\alpha|$ 这样的说法是有意义的. 更进一步, 我们知道任何一个良序集的子集在原良序排列诱导的排列下也是良序的.

正如我们对基数做的讨论一样, 我们现在要比较序数的大小. 令 M 是一个良序集, $m \in M$, 则称 $M_m = \{x \in M : x < m\}$ 是由 m

确定的 (初始) 分割集. 如果存在 m 使得 $N = M_m$, 则 N 是 M 的分割集. 因此, 特别地我们有, 如果 m 是 M 的第一个元素, 则 M_m 是空集. 现在我们令 μ 和 ν 分别是良序集 M 和 N 的序数. 如果 M 同 N 的一个分割集相似, 我们就称 μ 比 ν 小, $\mu < \nu$. 根据传递性, 我们从 $\mu < \nu, \nu < \pi$ 可以推出 $\mu < \pi$, 因为在一个相似映射下一个分割集是映满另一个分割集的.

$\{1,2,3,\cdots\}$ 的序数比 $\{1,3,5,\cdots,2,4,6,\cdots\}$ 的序数更小.

显然对于有限集, $m < n$ 和一般意义上的大小是等价的. 我们用 ω 表示由大小关系排序得到的 $\mathbb{N} = \{1,2,3,4,\cdots\}$ 的序数. 考虑任意有限 n 的分割集 $\mathbb{N}_{n+1}$, 我们有 $n < \omega$. 接下来我们将证明对于任意无限集的序数 α, 不等式 $\omega \leqslant \alpha$ 成立. 事实上, 如果无限良序集 M 有序数 α, 则 M 包含第一个元素 m_1, 集合 $M\backslash\{m_1\}$ 包含第一个元素 m_2, 集合 $M\backslash\{m_1,m_2\}$ 包含第一个元素 m_3. 继续这种操作, 我们得到 M 中的序列 $m_1 < m_2 < m_3 < \cdots$. 如果 $M = \{m_1,m_2,m_3,\cdots\}$, 则 M 同 $\mathbb{N}$ 相似, 且有 $\alpha = \omega$. 另一方面, 如果 $M\backslash\{m_1,m_2,\cdots\}$ 是非空的, 则其包含第一个元素 m, 则我们知道 $\mathbb{N}$ 相似于 M_m 的分割集, 由定义我们知道 $\omega < \alpha$.

现在我们要陈述三个关于序数的基本结果 (由于证明比较简单, 我们在这里不给出证明). 第一个结果陈述了所有序数 μ 都有一个标准的良序集合代表 W_μ.

命题 1. 令 μ 是一个序数且用 W_μ 表示比 μ 小的序数构成的集合, 则以下两点成立:
(i) 集合 W_μ 中的元素两两可以比较.
(ii) 如果我们根据大小关系将 W_μ 排序, 则 W_μ 是良序的且其序数是 μ.

命题 2. 任何两个序数 μ 和 ν 满足且仅满足以下条件之一: $\mu < \nu$, $\mu = \nu$, 或者 $\mu > \nu$.

命题 3. 任何序数构成的集合 (根据序数大小关系排序) 是良序的.

说了这么多序数的问题, 让我们回到基数的问题上来. 令 $\mathbf{m}$ 是基数, 且用 $O_{\mathbf{m}}$ 表示所有满足 $|\mu| = \mathbf{m}$ 的序数 μ 构成的集合. 根据命题 3, 我们知道在 $O_{\mathbf{m}}$ 存在一个最小的序数 $\omega_{\mathbf{m}}$, 我们将其称为 $\mathbf{m}$ 的*初始序数*. 举个例子, ω 是基数 $\aleph_0$ 的初始序数.

有了上述准备, 我们现在可以证明本章的一些基本结果了.

命题 4. 对于任何基数 $\mathbf{m}$, 存在紧接其后的更大的基数.

■ **证明.** 我们已经知道存在比 $\mathbf{m}$ 更大的基数 $\mathbf{n}$. 考虑所有比 $\mathbf{m}$ 大的基数构成的集合 $\mathcal{K}$ 且 $\mathcal{K}$ 至多和 $\mathbf{n}$ 一样大. 我们将每个 $\mathbf{p}\in\mathcal{K}$ 与其初始序数 $\omega_{\mathbf{p}}$ 联系起来. 在这些初始序数中存在一个最小的序数 (命题 3), 则这个对应的序数就是 $\mathcal{K}$ 中最小的序数, 因此它是紧跟 $\mathbf{m}$ 之后的更大的序数.

命题 5. *无限集 M 的基数是 $\mathbf{m}$, 根据初始序数 $\omega_{\mathbf{m}}$ 使其良序, 则 M 没有最后一个元素.*

■ **证明.** 事实上, 如果 M 有最后一个元素 m, 则分割集 M_m 有序数 $\mu<\omega_{\mathbf{m}}$ 且 $|\mu|=\mathbf{m}$, 这就与 $\omega_{\mathbf{m}}$ 的定义矛盾了.

我们最后需要的是一个比可数个可数集合之并是可数的这个结论更强的结果. 下面我们考虑的是任意可数集族.

命题 6. *设 $\{A_\alpha\}$ 是由可数集合 A_α 构成的基数为 $\mathbf{m}$ 的集合族, 其中 $\mathbf{m}$ 是无限基数, 则并 $\bigcup\limits_\alpha A_\alpha$ 的基至多是 $\mathbf{m}$.*

■ **证明.** 我们可以假设 A_α 是两并不相交的, 因为这样只会使 $\bigcup\limits_\alpha A_\alpha$ 的基数增加. 设 M 是基为 $|M|=\mathbf{m}$ 的指标集, 且根据初始序数 $\omega_{\mathbf{m}}$ 将其良序化. 我们用可数集合 $B_\alpha=\{b_{\alpha 1}=\alpha,b_{\alpha 2},b_{\alpha 3},\cdots\}$ 去替代每个 $\alpha\in M$, 并且根据 ω 将 B_α 排序, 称这样得到的新集合是 $\widetilde{M}$. 规定对于 $\alpha<\beta$ 有 $b_{\alpha i}<b_{\beta j}$ 以及 $i<j$ 有 $b_{\alpha i}<b_{\alpha j}$, 则 $\widetilde{M}$ 也是良序的. 令 $\widetilde{\mu}$ 是 $\widetilde{M}$ 的序数. 因为 M 是 $\widetilde{M}$ 的子集, 由前面的一个结论我们知道 $\mu\leqslant\widetilde{\mu}$. 如果 $\mu=\widetilde{\mu}$, 则 M 相似于 $\widetilde{M}$, 且如果 $\mu<\widetilde{\mu}$, 则 M 相似于 $\widetilde{M}$ 的分割集. 因为 M 的序数 $\omega_{\mathbf{m}}$ 没有最后一个元素 (命题 5), 我们知道 M 在两种情况下都是相似于可数集合 B_β 的并, 故两者具有相同的基.

余下的证明就比较简单了. 设 $\varphi:\bigcup B_\beta\longrightarrow M$ 是一个双射且令 $\varphi(B_\beta)=\{\alpha_1,\alpha_2,\alpha_3,\cdots\}$. 用 A_{α_i} 去替代 α_i 并且考虑并 $\bigcup A_{\alpha_i}$. 因为 $\bigcup A_{\alpha_i}$ 是可数个可数集之并 (故可数) , 我们知道 B_β 和 $\bigcup A_{\alpha_i}$ 有相同的基. 换言之, 对于所有 β, 在 B_β 和 $\bigcup A_{\alpha_i}$ 存在一个双射, 所以 ψ 是从 $\bigcup B_\beta$ 到 $\bigcup A_\alpha$ 的双射. 但是, $\psi\varphi^{-1}$ 给出了从 M 到 $\bigcup A_\alpha$ 的双射, 所以 $|\bigcup A_\alpha|=\mathbf{m}$. □

参考文献

[1] L. E. J. Brouwer: *Beweis der Invarianz der Dimensionszahl,* Math.

Annalen **70** (1911), 161-165.

[2] N. Calkin & H. Wilf: *Recounting the rationals,* Amer. Math. Monthly **107** (2000), 360-363.

[3] P. Cohen: *Set Theory and the Continuum Hypothesis,* W. A. Benjamin, New York 1966.

[4] P. Erdős: *An interpolation problem associated with the continuum hypothesis,* Michigan Math. J. **11** (1964), 9-10.

[5] E. Kamke: *Theory of Sets,* Dover Books 1950.

[6] M. A. Stern: *Ueber eine zahlentheoretische Funktion,* Journal für die reine und angewandte Mathematik **55** (1858), 193-220.



“无穷多更大的基数”

不等式颂

第 17 章

分析中充满了不等式, Hardy, Littlewood 和 Pólya 的名著《不等式》是一个很好的见证. 让我们挑出两个最基本的不等式以及它们各自的两个运用, 看一看 George Pólya 所认为的最佳证明.

我们的第一个不等式是由 Cauchy, Schwarz 以及 Buniakowski 独立证明的.

定理 I (Cauchy-Schwarz 不等式)

设 $\langle a, b\rangle$ 是实向量空间 V 的内积 (范数是$|a|^2 := \langle a, a\rangle$). 那么

$$\langle a, b\rangle^2 \leqslant |a|^2|b|^2$$

对任意向量 $a, b \in V$ 都成立, 其中等式成立当且仅当 a 和 b 是线性相关的.

■ **证明.** 下面的 (民间的) 证明也许是最短的. 考虑变量 x 的二次方程

$$|xa + b|^2 = x^2|a|^2 + 2x\langle a, b\rangle + |b|^2.$$

我们可以假设 $a \neq 0$. 如果 $b = \lambda a$, 则显然有 $\langle a, b\rangle^2 = |a|^2|b|^2$. 另一方面, 如果 a 和 b 是线性无关的, 则对于任意 x 有 $|xa + b|^2 > 0$, 因此判别式 $\langle a, b\rangle^2 - |a|^2|b|^2$ 是小于 0 的. □

我们下个例子是关于调和平均值、几何平均值以及算术平均值的不等式:

定理 II (调和、几何和算术平均值)

令 $a_1, \cdots, a_n$ 是正实数, 则

$$\frac{n}{\frac{1}{a_1} + \cdots + \frac{1}{a_n}} \leqslant \sqrt[n]{a_1 a_2 \cdots a_n} \leqslant \frac{a_1 + \cdots + a_n}{n}$$

两边等式成立当且仅当所有的 a_i 相等.

■ **证明.** 以下漂亮的非标准归纳证明是 Cauchy 给出的 (参见 [7]). 用 $P(n)$ 表示上面的第二个不等式, 它可以写成以下形式:

$$a_1 a_2 \cdots a_n \leqslant \left(\frac{a_1 + \cdots + a_n}{n}\right)^n.$$

对于 $n=2$, 我们有 $a_1a_2 \leqslant (\frac{a_1+a_2}{2})^2 \iff (a_1-a_2)^2 \geqslant 0$, 故第二个不等式成立. 现在我们分下列两步进行:

(A) $P(n) \Longrightarrow P(n-1)$

(B) $P(n)$ 且 $P(2) \Longrightarrow P(2n)$

显然, 由此可以推出结论.

为了证明**(A)**, 令 $A := \sum_{k=1}^{n-1} \frac{a_k}{n-1}$, 则

$$\Big(\prod_{k=1}^{n-1} a_k\Big)A \overset{P(n)}{\leqslant} \left(\frac{\sum_{k=1}^{n-1} a_k + A}{n}\right)^n = \left(\frac{(n-1)A+A}{n}\right)^n = A^n$$

故有 $\prod_{k=1}^{n-1} a_k \leqslant A^{n-1} = \left(\frac{\sum_{k=1}^{n-1} a_k}{n-1}\right)^{n-1}$.

对于**(B)**, 我们有

$$\prod_{k=1}^{2n} a_k = \Big(\prod_{k=1}^{n} a_k\Big)\Big(\prod_{k=n+1}^{2n} a_k\Big) \overset{P(n)}{\leqslant} \Big(\sum_{k=1}^{n} \frac{a_k}{n}\Big)^n \Big(\sum_{k=n+1}^{2n} \frac{a_k}{n}\Big)^n$$

$$\overset{P(2)}{\leqslant} \left(\frac{\sum_{k=1}^{2n} \frac{a_k}{n}}{2}\right)^{2n} = \left(\frac{\sum_{k=1}^{2n} a_k}{2n}\right)^{2n}.$$

等式的条件是非常容易导出的.

通过考虑 $\frac{1}{a_1}, \cdots, \frac{1}{a_n}$, 我们得到左边关于调和平均值和几何平均值的不等式. □

■ **另一个证明.** 在算术 — 几何平均值不等式的许多其他的证明中 (专著 [2] 列出了至少 50 种), 让我们来看看最近才由 Alzer 给出的一个惊人的证明. 事实上, 这个证明可以推出更强的不等式. 对于任何正数 $a_1, \cdots, a_n, p_1, \cdots, p_n$ 且 $\sum_{i=1}^n p_i = 1$, 有如下不等式成立:

$$a_1^{p_1} a_2^{p_2} \cdots a_n^{p_n} \leqslant p_1a_1 + p_2a_2 + \cdots + p_na_n.$$

让我们用 A 表示右边的表达式, 用 G 表示左边的表达式. 我们可以假定 $a_1 \leqslant \cdots \leqslant a_n$. 显然 $a_1 \leqslant G \leqslant a_n$, 因此必存在某个 k 使得 $a_k \leqslant G \leqslant a_{k+1}$. 从而得到

$$\sum_{i=1}^{k} p_i \int_{a_i}^{G} \Big(\frac{1}{t} - \frac{1}{G}\Big)\,dt + \sum_{i=k+1}^{n} p_i \int_{G}^{a_i} \Big(\frac{1}{G} - \frac{1}{t}\Big)\,dt \geqslant 0, \qquad (1)$$

因为每个被积函数都是大于 0 的. 重写 (1), 我们得到

$$\sum_{i=1}^{n} p_i \int_G^{a_i} \frac{1}{G}\,dt \;\geqslant\; \sum_{i=1}^{n} p_i \int_G^{a_i} \frac{1}{t}\,dt,$$

其中左边等于

$$\sum_{i=1}^{n} p_i \frac{a_i - G}{G} = \frac{A}{G} - 1,$$

而右边等于

$$\sum_{i=1}^{n} p_i(\log a_i - \log G) = \log \prod_{i=1}^{n} a_i^{p_i} - \log G = 0.$$

我们得到 $\frac{A}{G} - 1 \geqslant 0$, 这正是 $A \geqslant G$. 对于等式情形, (1) 中的所有积分都必须是 0, 这蕴含着 $a_1 = \cdots = a_n = G$. □

我们的第一个应用是 Laguerre 给出的 (参见 [7]) 关于多项式根的位置的一个漂亮结果.

定理 1. *设多项式 $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 的所有根都是实数, 则这些根都分布在以如下两数为左右端点的区间内:*

$$-\frac{a_{n-1}}{n} \pm \frac{n-1}{n}\sqrt{a_{n-1}^2 - \frac{2n}{n-1}a_{n-2}}\,.$$

■ **证明.** 令 y 是一个根且 $y_1, \cdots, y_{n-1}$ 是其他的根, 则多项式可以写成 $(x-y)(x-y_1)\cdots(x-y_{n-1})$. 因此通过比较系数我们得到

$$\begin{aligned} -a_{n-1} &= y + y_1 + \cdots + y_{n-1}, \\ a_{n-2} &= y(y_1 + \cdots + y_{n-1}) + \sum_{i<j} y_i y_j, \end{aligned}$$

从而

$$a_{n-1}^2 - 2a_{n-2} - y^2 = \sum_{i=1}^{n-1} y_i^2.$$

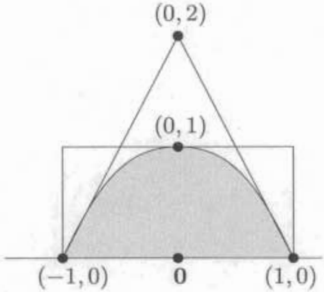
将 Cauchy 不等式运用到 $(y_1, \cdots, y_{n-1})$ 和 $(1, \cdots, 1)$ 上, 可以得到:

$$\begin{aligned} (a_{n-1} + y)^2 &= (y_1 + y_2 + \cdots + y_{n-1})^2 \\ &\leqslant (n-1)\sum_{i=1}^{n-1} y_i^2 = (n-1)(a_{n-1}^2 - 2a_{n-2} - y^2), \end{aligned}$$

或者

$$y^2 + \frac{2a_{n-1}}{n}y + \frac{2(n-1)}{n}a_{n-2} - \frac{n-2}{n}a_{n-1}^2 \leqslant 0.$$

故 y (和所有的 y_i) 都在上述二次方程的两根之间, 且它们的根就是界. □



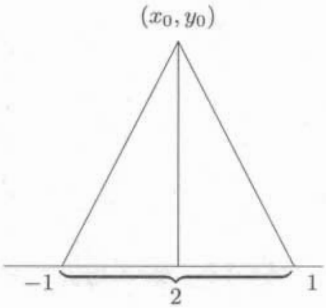
从抛物线的一个基本性质开始, 我们来看看第二个应用. 考虑 $x = -1$ 和 $x = 1$ 之间的抛物线 $f(x) = 1 - x^2$. 我们将 $f(x)$ 与其切三角形和切矩形联系起来 (如图所示).

我们发现阴影部分的面积 $A = \int_{-1}^{1}(1-x^2)dx$ 等于 $\frac{4}{3}$, 且三角形的面积 T 和矩形的面积 R 是等于 2 的. 因此 $\frac{T}{A} = \frac{3}{2}$ 且 $\frac{R}{A} = \frac{3}{2}$.

在一篇精彩的论文中, Paul Erdős 和 Tibor Gallai 提出这样一个问题: 设 $f(x)$ 是 $-1 < x < 1$ 上满足 $f(x) > 0$ 的任意 n 次实多项式, 且有 $f(-1) = f(1) = 0$, 这种情况下会发生什么? A 的面积是 $\int_{-1}^{1} f(x)dx$. 假设 $f(x)$ 在 $(-1, 1)$ 内达到的最大值是 b, 则 $R = 2f(b)$. 计算 $f(x)$ 在 -1 和 1 处的切线, 得到 (参见下列方框中的内容):

$$T = \frac{2f'(1)f'(-1)}{f'(1) - f'(-1)}, \tag{2}$$

当 $f'(1)$ 或 $f'(-1) = 0$ 时, 有 $T = 0$.



切三角形

切三角形的面积 T 是 y_0, 其中 (x_0, y_0) 是两条切线的交点. 切线方程是 $y = f'(-1)(x+1)$ 和 $y = f'(1)(x-1)$, 因此

$$x_0 = \frac{f'(1) + f'(-1)}{f'(1) - f'(-1)},$$

故

$$y_0 = f'(1)\left(\frac{f'(1) + f'(-1)}{f'(1) - f'(-1)} - 1\right) = 2\frac{f'(1)f'(-1)}{f'(1) - f'(-1)}.$$

一般而言, 对于 $\frac{T}{A}$ 和 $\frac{R}{A}$ 没有非平凡的界. 为了阐述这个, 我们令 $f(x) = 1 - x^{2n}$, 则 $T = 2n$, $A = \frac{4n}{2n+1}$, 故 $\frac{T}{A} > n$. 类似地, $R = 2$ 且 $\frac{R}{A} = \frac{2n+1}{2n}$, 当 n 趋于无穷时该值为 1.

但是 Erdős 和 Gallai 证明了对只有实数根的多项式才存在这样的界.

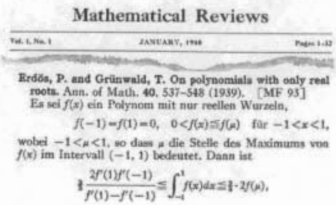
定理 2. 令 $f(x)$ 是一个只有实根的 $n \geqslant 2$ 次实多项式, 满足在开区

间 $-1 < x < 1$ 上有 $f(x) > 0$ 以及 $f(-1) = f(1) = 0$. 那么

$$\frac{2}{3}T \leqslant A \leqslant \frac{2}{3}R,$$

且只有当 $n = 2$ 时两种情形的等号成立.

Erdős 和 Gallai 用一个非常复杂的归纳证明了这个结论. 1940 年, 在Mathematical Reviews的第一期的第一页关于他这篇论文的评论中, George Pólya 解释了第一个不等式怎样还可以由几何 — 算术不等式得到, 这篇评论的严谨认真堪称范例, 同时也是一个天书证明.


Mathematical Reviews

Vol. 1, No. 1　JANUARY, 1940　Pages 1-32

Erdős, P. and Grünwald, T. On polynomials with only real roots. Ann. of Math. **40**, 537–548 (1939). [MF 93]
Es sei $f(x)$ ein Polynom mit nur reellen Wurzeln,

$$f(-1)=f(1)=0,\quad 0<f(x)\leqq f(\mu)\quad \text{für } -1<x<1,$$

wobei $-1<\mu<1$, so dass μ die Stelle des Maximums von $f(x)$ im Intervall $(-1, 1)$ bedeutet. Dann ist

$$\tfrac{2}{3}\frac{2f'(1)f'(-1)}{f'(1)-f'(-1)}\leqq\int_{-1}^{1}f(x)dx\leqq\tfrac{2}{3}\cdot 2f(\mu).$$

■ **$\frac{2}{3}T \leqslant A$ 的证明.** 因为 $f(x)$ 只有实数根, 且所有根都不在区间 $(-1, 1)$ 内, 该多项式可以被写成 (除在最后删去的正常数因子之外) 以下形式

$$f(x) = (1-x^2)\prod_i(\alpha_i - x)\prod_j(\beta_j + x), \qquad (3)$$

其中 $\alpha_i \geqslant 1, \beta_j \geqslant 1$. 故

$$A = \int_{-1}^{1}(1-x^2)\prod_i(\alpha_i - x)\prod_j(\beta_j + x)dx.$$

做替换 $x \longmapsto -x$, 我们得到

$$A = \int_{-1}^{1}(1-x^2)\prod_i(\alpha_i + x)\prod_j(\beta_j - x)dx,$$

因此根据算术 — 几何平均值不等式 (注意到乘积中的所有因子都 $\geqslant 0$)

$$\begin{aligned}
A &= \int_{-1}^{1}\frac{1}{2}\Big[(1-x^2)\prod_i(\alpha_i - x)\prod_j(\beta_j + x) + \\
&\qquad\qquad (1-x^2)\prod_i(\alpha_i + x)\prod_j(\beta_j - x)\Big]dx \\
&\geqslant \int_{-1}^{1}(1-x^2)\Big(\prod_i(\alpha_i^2 - x^2)\prod_j(\beta_j^2 - x^2)\Big)^{1/2}dx \\
&\geqslant \int_{-1}^{1}(1-x^2)\Big(\prod_i(\alpha_i^2 - 1)\prod_j(\beta_j^2 - 1)\Big)^{1/2}dx \\
&= \frac{4}{3}\Big(\prod_i(\alpha_i^2 - 1)\prod_j(\beta_j^2 - 1)\Big)^{1/2}.
\end{aligned}$$

让我们计算 $f'(1)$ 和 $f'(-1)$. (我们可以假设 $f'(-1), f'(1) \neq 0$, 因为如果 $T=0$ 则不等式 $\frac{2}{3}T \leqslant A$ 就变成了平凡形式.) 根据 (3) 我们看到

$$f'(1) = -2\prod_i(\alpha_i - 1)\prod_j(\beta_j + 1),$$

且类似地

$$f'(-1) = 2\prod_i(\alpha_i + 1)\prod_j(\beta_j - 1).$$

因此我们得到结论

$$A \geqslant \frac{2}{3}(-f'(1)f'(-1))^{1/2}.$$

在 $-f'(1)$ 和 $f'(1)$ 上运用调和 — 几何平均值不等式, 根据 (2) 我们得到结论:

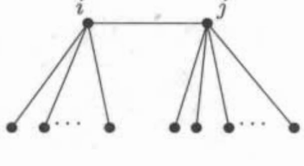
$$A \geqslant \frac{2}{3}\frac{2}{\frac{1}{-f'(1)}+\frac{1}{f'(-1)}} = \frac{4}{3}\frac{f'(1)f'(-1)}{f'(1)-f'(-1)} = \frac{2}{3}T,$$

通过分析不等式中等号成立的情形, 读者很容易得到定理的最后部分. □

请读者自己寻找定理 2 中第二个不等式的类似证明.

当然, 分析学毕竟就只讨论不等式, 但图论中存在一个运用不等式而得到出乎意料的结论的例子. 我们将在第 32 章中讨论 Turán 定理. 如下是其最简单的形式:

定理 3. 设 G 是一个具有 n 个顶点且其中没有三角形的图. 那么 G 至多有 $\frac{n^2}{4}$ 条边且等式成立当且仅当 n 是偶数且 G 是完全二部图 $K_{n/2,n/2}$.



■ **第一个证明.** 这个运用 Cauchy 不等式的证明是 Mantel 给出的. 令 G 的顶点集是 $V=\{1,\cdots,n\}$, 边集是 E. 用 d_i 表示顶点 i 的度, 因此 $\sum_{i\in V} d_i = 2|E|$ (参见双重计数那章). 设 ij 是一条边. 由于 G 没有三角形, 我们知道 $d_i + d_j \leqslant n$, 因为没有顶点同时与 i 和 j 相连.

从而有以下结论:

$$\sum_{ij\in E}(d_i + d_j) \leqslant n|E|.$$

注意到 d_i 在和里只出现 d_i 次, 因此我们得到

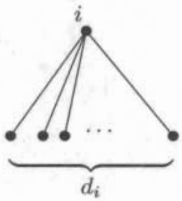
$$n|E| \geqslant \sum_{ij\in E}(d_i + d_j) = \sum_{i\in V} d_i^2,$$

且将 Cauchy 不等式运用到向量 $(d_1,\cdots,d_n)$ 和 $(1,\cdots,1)$ 上, 有:

$$n|E| \geqslant \sum_{i\in V} d_i^2 \geqslant \frac{(\sum d_i)^2}{n} = \frac{4|E|^2}{n},$$

故得到结论. 关于等式情形, 对任意 i,j 我们得到 $d_i = d_j$, 进一步有 $d_i = \frac{n}{2}$ (因为 $d_i + d_j = n$) . 由于 G 是没有三角形的, 故可以立即得到 $G = K_{n/2,n/2}$. □

■ **第二个证明.** 这个用算术平均值和几何平均值的证明是一个民间的天书证明. 令 α 是最大独立集 A 的基数, 且令 $\beta = n - \alpha$. 由于 G 是没有三角形的. 顶点 i 的邻点构成了一个独立集, 我们推断出对于任意 i 有 $d_i \leqslant \alpha$.



基数为 β 的集合 $B = V\setminus A$ 与 G 中的每条边都相遇. 根据 B 中的顶点来数 G 的边数, 我们得到 $|E| \leqslant \sum_{i\in B} d_i$. 由算术 — 几何平均值不等式我们得到:

$$|E| \leqslant \sum_{i\in B} d_i \leqslant \alpha\beta \leqslant \left(\frac{\alpha+\beta}{2}\right)^2 = \frac{n^2}{4},$$

并且同样地, 等号情形是易证的.

参考文献

[1] H. Alzer: *A proof of the arithmetic mean-geometric mean inequality,* Amer. Math. Monthly **103** (1996), 585.

[2] P. S. Bullen, D. S. Mitrinovics & P. M. Vasić: *Means and their Inequalities,* Reidel, Dordrecht 1988.

[3] P. Erdős & T. Grünwald: *On polynomials with only real roots,* Annals Math. **40** (1939), 537-548.

[4] G. H. Hardy, J. E. Littlewood & G. Pólya: *Inequalities,* Cambridge University Press, Cambridge 1952.

[5] W. Mantel: *Problem 28,* Wiskundige Opgaven **10** (1906), 60-61.

[6] G. Pólya: *Review of* [3], Mathematical Reviews **1** (1940), 1.

[7] G. Pólya & G. Szegő: *Problems and Theorems in Analysis, Vol. I,* Springer-Verlag, Berlin Heidelberg New York 1972/78; Reprint 1998.

且由 Cauchy 不等式运用到向量 $(d_1,\cdots,d_n)$ 和 $(1,\cdots,1)$ 上,有

$$n|E| \geqslant \sum_{i\in V} d_i^2 \geqslant \frac{(\sum d_i)^2}{n} = \frac{4|E|^2}{n},$$

这就得到结论. 关于等式情形, 对任意 ij 我们得到 $d_i = d_j$, 进一步有 $d_i = \frac{n}{2}$ (因为 $d_i + d_j = n$). 由于 G 是没有三角形的, 故可以立即得到 $G = K_{n/2,n/2}$. □

■ 第二个证明. 这个用算术平均值和几何平均值的证明是一个民间的大卫证明. 令 α 是最大独立集 A 的基数, 且令 $\beta = n - \alpha$. 由于 G 是没有三角形的, 顶点 i 的邻域构成了一个独立集, 我们推断出对于任意 i 有 $d_i \leqslant \alpha$.

集合 $B = V\backslash A$ 与 G 中的每条边都相遇, 根据 B 中的顶点来数 G 的边数, 我们得到 $|E| \leqslant \sum_{i\in B} d_i$. 由算术—几何平均值不等式我们得到

$$|E| \leqslant \sum_{i\in B} d_i \leqslant \alpha\beta \leqslant \left(\frac{\alpha+\beta}{2}\right)^2 = \frac{n^2}{4},$$

并且同样地, 等号情形是易证的.

参考文献

[1] H. Alzer: *A proof of the arithmetic mean-geometric mean inequality*, Amer. Math. Monthly 103(1996), 585.

[2] P. S. Bullen, D. S. Mitrinovics & P. M. Vasić: *Means and their Inequalities*, Reidel, Dordrecht 1988.

[3] P. Erdős & T. Grünwald: *On polynomials with only real roots*, Annals Math. 40(1939), 537-548.

[4] G. H. Hardy, J. E. Littlewood & G. Pólya: *Inequalities*, Cambridge University Press, Cambridge 1952.

[5] W. Mantel: *Problem 28*, Wiskundige Opgaven 10(1906), 60-61.

[6] G. Pólya: *Review of [3]*, Mathematical Reviews 1(1940), 1.

[7] G. Pólya & G. Szegő: *Problems and Theorems in Analysis, Vol. I*, Springer-Verlag, Berlin Heidelberg New York 1972/78; Reprint 1998.

关于多项式的 Pólya 定理

第 18 章

在 George Pólya 对分析所作的诸多贡献中, Erdős 最喜欢以下结论, 一方面是因其出乎意料的结果, 另一方面也因其漂亮的证明. 设

$$f(z) = z^n + b_{n-1}z^{n-1} + \cdots + b_0$$

是一个次数为 $n \geqslant 1$ 且首项系数为 1 的复多项式. 将 $f(z)$ 与集合

$$\mathcal{C} := \{z \in \mathbb{C} : |f(z)| \leqslant 2\}$$

联系起来, 即 $\mathcal{C}$ 是那些被 f 映到复平面上以原点为圆心以 2 为半径的圆内的点构成的集合. 因此当 $n = 1$ 时, 区域 $\mathcal{C}$ 恰是一个直径为 4 的圆盘.

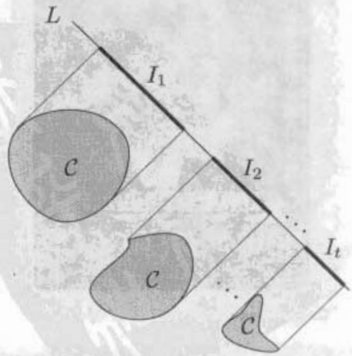


George Pólya

通过一个非常简单的论证, Pólya 发现了以下关于集合 $\mathcal{C}$ 的漂亮性质:

取复平面中任何一条直线 L 并且考虑 $\mathcal{C}$ 在 L 上的正交投影 $\mathcal{C}_L$, 则任何这种投影的总长度不超过 4.

所有投影 $\mathcal{C}_L$ 的长度之和不超过 4 是什么意思? 我们将会看到 $\mathcal{C}_L$ 是由有限个互不相交的区间 $I_1, \cdots, I_t$ 组成, 且上述条件表明 $\ell(I_1) + \cdots + \ell(I_t) \leqslant 4$, 其中 $\ell(I_j)$ 表示区间的长度.



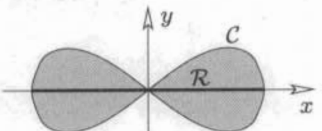
通过旋转平面, 我们知道只需证明当 L 是复平面上实数轴的情形. 有了这些注解, 以下我们将陈述 Pólya 的结论.

定理 1. *假设 $f(z)$ 是一个次数至少为 1 且首项系数为 1 的复数多项式. 我们定义 $\mathcal{C} = \{z \in \mathbb{C} : |f(z)| \leqslant 2\}$ 并且令 $\mathcal{R}$ 是 $\mathcal{C}$ 在实数轴上的正交投影. 那么存在可以覆盖 $\mathcal{R}$ 的区间 $I_1, \cdots, I_t$ 满足*

$$\ell(I_1) + \cdots + \ell(I_t) \leqslant 4.$$

显然 $n = 1$, 这个定理可以达到上界. 为了获得关于这个定理的更多直观理解, 让我们来看看同样达到上界 4 的多项式 $f(z) = z^2 - 2$. 如果 $z = x + iy$ 是一个复数, 则 x 是其在实数轴上的正交投影. 因此:

$$\mathcal{R} = \{x \in \mathbb{R} : x + iy \in \mathcal{C} \text{ 对于某些 } y\}.$$

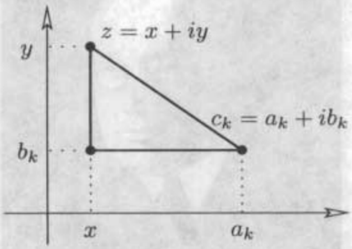


$f(z) = z^2 - 2$

读者可以很容易证明对于 $f(z) = z^2 - 2$, 我们有 $x + iy \in \mathcal{C}$ 当且仅当

$$(x^2 + y^2)^2 \leqslant 4(x^2 - y^2).$$

由上式得到 $x^4 \leqslant (x^2+y^2)^2 \leqslant 4x^2$, 故 $x^2 \leqslant 4$, 即 $|x| \leqslant 2$. 另一方面, 对于任意 $z = x \in \mathbb{R}(|x| \leqslant 2)$ 满足 $|z^2 - 2| \leqslant 2$, 我们发现 $\mathcal{R}$ 正好是长度为 4 的区间 $[-2, 2]$.



作为证明的第一步, 我们令 $f(z) = (z-c_1)\cdots(z-c_n)$ $(c_k = a_k + ib_k)$, 且考虑实多项式 $p(x) = (x-a_1)\cdots(x-a_n)$. 设 $z = x + iy \in \mathcal{C}$, 则由 Pythagoras (勾股) 定理我们得到:

$$|x - a_k|^2 + |y - b_k|^2 = |z - c_k|^2.$$

因此对于任意 k 我们有 $|x - a_k| \leqslant |z - c_k|$, 即

$$|p(x)| = |x - a_1|\cdots|x - a_n| \leqslant |z - c_1|\cdots|z - c_n| = |f(z)| \leqslant 2.$$

故我们知道 $\mathcal{R}$ 包含在 $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \leqslant 2\}$ 中, 并且如果我们可以证明后者可以被总长度小于 4 的区间覆盖, 则定理 1 得证. 因此, 定理 1 的主要证明来自于下述结果.

定理 2. *假设 $p(x)$ 是一个次数为 $n \geqslant 1$, 首项系数为 1 且所有根都是实数的实多项式. 那么集合 $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \leqslant 2\}$ 可以被总长度不超过 4 的一些区间所覆盖.*



Pavnuty Chebyshev 的头像在前苏联 1946 年发行的邮票上

根据 Pólya 的论文 [2], 定理 2 是由如下著名的 Chebyshev 定理得到的. 为了完备本章, 我们在附录里给出了一个证明 (源于 Pólya 和 Szegő 的优美展示).

Chebyshev 定理.
令 $p(x)$ 是次数为 $n \geqslant 1$ 且首项系数为 1 的实多项式, 则有

$$\max_{-1 \leqslant x \leqslant 1} |p(x)| \geqslant \frac{1}{2^{n-1}}.$$

首先我们给出以下一个直接的结果.

推论. *令 $p(x)$ 是次数为 $n \geqslant 1$ 且首项系数为 1 的实多项式. 假设对于任意属于区间 $[a, b]$ 的 x 都有 $|p(x)| \leqslant 2$ 成立, 那么 $b - a \leqslant 4$.*

■ **证明.** 考虑置换 $y = \frac{2}{b-a}(x-a)-1$, 这个映射将 x 的一个区间 $[a,b]$ 映满 y 的一个区间 $[-1,1]$. 对应的多项式

$$q(y) = p(\tfrac{b-a}{2}(y+1)+a)$$

的首项系数是 $(\frac{b-a}{2})^n$ 且满足

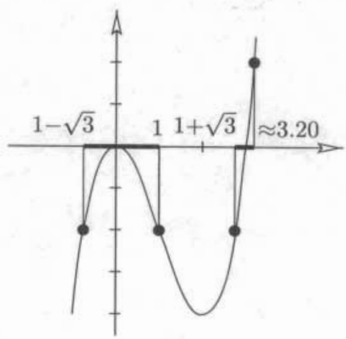
$$\max_{-1\leqslant y\leqslant 1} |q(y)| = \max_{a\leqslant x\leqslant b} |p(x)|.$$

根据 Chebyshev 定理, 我们推导出

$$2 \geqslant \max_{a\leqslant x\leqslant b} |p(x)| \geqslant (\tfrac{b-a}{2})^n \tfrac{1}{2^{n-1}} = 2(\tfrac{b-a}{4})^n,$$

故 $b-a \leqslant 4$. □

这个推论使我们与定理 2 非常接近了. 如果集合 $\mathcal{P} = \{x : |p(x)| \leqslant 2\}$ 是一个区间, 则 $\mathcal{P}$ 的长度至多是 4. 但是集合 $\mathcal{P}$ 可能不是一个区间, 这里我们给出一个例子, 在这个例子中 $\mathcal{P}$ 包含两个区间.

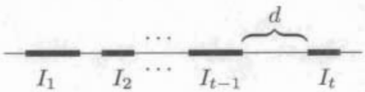


对于多项式 $p(x) = x^2(x-3)$ 我们得到 $\mathcal{P} = [1-\sqrt{3}, 1] \cup [1+\sqrt{3}, \approx 3.2]$

我们可以对 $\mathcal{P}$ 说些什么呢? 因为 $p(x)$ 是一个连续函数, 我们知道无论如何 $\mathcal{P}$ 是一系列不相交的闭区间 $I_1, I_2, \cdots$ 的并, 且 $p(x)$ 将每个区间 I_j 的两个端点映成 2 或 -2. 这就说明了只可能有有限个区间 $I_1, \cdots, I_t$, 因为 $p(x)$ 只能将有限个点映成 2 或 -2.

Pólya 精彩的想法就是要构造另外一个次数为 n, 首项系数为 1 的多项式 $\tilde{p}(x)$, 使得 $\widetilde{\mathcal{P}} = \{x : |\tilde{p}(x)| \leqslant 2\}$ 是长度至少为 $\ell(I_1)+\cdots+\ell(I_t)$ 的区间. 上述推论证明了 $\ell(I_1)+\cdots+\ell(I_t) \leqslant \ell(\widetilde{\mathcal{P}}) \leqslant 4$, 这样我们就完成了证明.

■ **定理 2 的证明.** 设 $p(x) = (x-a_1)\cdots(x-a_n)$, $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \leqslant 2\} = I_1 \cup \cdots \cup I_t$, 并且使得 I_1 是最左边的区间, I_t 是最右边的区间. 首先我们要证每个区间 I_j 都包含 $p(x)$ 的一个根. 我们知道 $p(x)$ 将 I_j 的两个端点映到 2 或 -2. 如果一个端点的函数值是 2 而另一个是 -2, 则 I_j 中肯定存在多项式的根. 因此我们假定两个端点的函数值都是 $p(x) = 2$ (对于 $p(x) = -2$ 的情形是类似的). 假设 $b \in I_j$ 是 I_j 中 $p(x)$ 的函数值最小的点, 则 $p'(b) = 0$ 且 $p''(b) \geqslant 0$. 如果 $p''(b) = 0$, 则 b 是 $p'(x)$ 的重根, 由下页方框中的事实 1 我们知道 b 也是 $p(x)$ 的根. 另一方面, 如果 $p''(b) > 0$, 则我们可以由事实 2 推出 $p(b) \leqslant 0$. 故不管 $p(b) = 0$ 还是 $p(b) < 0$, 我们都可以找到一个介于 b 与 I_j 的其中一个端点之间的根.



这里我们将要阐述定理最后的思想. 令 $I_1, \cdots, I_t$ 是如上所述的区间, 并且假设最右边的区间 I_t 包含 $p(x)$ 的 m 个根 (按重数计算). 如果 $m = n$, 则 I_t 是唯一的区间 (以上我们已证明), 定理证毕. 因此假设 $m < n$, 并且令 d 是如图所示区间 I_{t-1} 和 I_t 之间的距离. 令 $b_1, \cdots, b_m$ 是包含在区间 I_t 内的 $p(x)$ 的根, $c_1, \cdots c_{n-m}$ 是剩下的根. 我们记 $p(x) = q(x)r(x)$, 其中 $q(x) = (x-b_1)\cdots(x-b_m)$, $r(x) = (x-c_1)\cdots(x-c_{n-m})$. 设 $p_1(x) = q(x+d)r(x)$, 则多项式 $p_1(x)$ 也是次数为 n, 首项系数为 1 的多项式. 对于任意 $x \in I_1 \cup \cdots \cup I_{t-1}$ 我们有 $|x+d-b_i| < |x-b_i|$ (对于任意 i), 因此 $|q(x+d)| < |q(x)|$. 从而得到以下不等式:

$$|p_1(x)| \leqslant |p(x)| \leqslant 2, \qquad 对\ x \in I_1 \cup \cdots \cup I_{t-1}.$$

另一方面, 如果 $x \in I_t$, 则我们知道 $|r(x-d)| \leqslant |r(x)|$, 故

$$|p_1(x-d)| = |q(x)||r(x-d)| \leqslant |p(x)| \leqslant 2,$$

这就表明了 $I_t - d \subseteq \mathcal{P}_1 = \{x : |p_1(x)| \leqslant 2\}$.

总之, 我们知道 $\mathcal{P}_1$ 包含 $I_1 \cup \cdots \cup I_{t-1} \cup (I_t - d)$ 且其总长度至少和 $\mathcal{P}$ 一样大. 注意到从 $p(x)$ 到 $p_1(x)$, 区间 I_{t-1} 和 $I_t - d$ 合并成一个区间. 我们得到结论: 由 $p_1(x)$ 的区间 $J_1, \cdots, J_s$ 组成的 $\mathcal{P}_1$ 的总长度至少是 $\ell(I_1) + \cdots + \ell(I_t)$, 且其最右端的区间 J_s 至少包括 $p_1(x)$ 的 m 个根. 重复这个过程至多 $t-1$ 次, 我们最后得到一个多项式 $\tilde{p}(x)$, 且 $\widetilde{\mathcal{P}} = \{x : |\tilde{p}(x)| \leqslant 2\}$ 是长度为 $\ell(\widetilde{\mathcal{P}}) \geqslant \ell(I_1) + \cdots \ell(I_t)$ 的区间, 这样我们就证明了定理. □

实根多项式的两个事实

设 $p(x)$ 是一个只有实根的非零次多项式.

事实 1. 如果 b 是 $p'(x)$ 的重根, 则 b 也是 $p(x)$ 的根.

■ **证明.** 令 $b_1 < \cdots < b_r$ 是 $p(x)$ 重数为 $s_1, \cdots, s_r$, $\sum_{j=1}^{r} s_j = n$ 的根. 根据 $p(x) = (x-b_j)^{s_j} h(x)$, 我们得到如果 $s_j \geqslant 2$, b_j 是 $p'(x)$ 的根, 且 b_j 是 $p'(x)$ 的重数为 $s_j - 1$ 的根. 进一步地, 在 b_1 和 b_2 之间存在 $p'(x)$ 的一个根, 在 b_2 和 b_3 之间存在另一个 ⋯⋯, 且在 b_{r-1} 和 b_r 之间还有一个, 并且所有的这些根都是单根, 因为 $\sum_{j=1}^{r}(s_j - 1) + (r-1)$ 已经是 $p'(x)$ 的次数 $n-1$ 了. 故 $p'(x)$ 的重根只能出现在 $p(x)$ 的根中. □

事实 2. 对于任意 $x \in \mathbb{R}$ 我们有 $p'(x)^2 \geqslant p(x)p''(x)$.

■ **证明.** 如果 $x = a_i$ 是 $p(x)$ 的一个根, 则上述不等式显然成立. 假设 x 不是根, 由求导准则得到以下式子:

$$p'(x) = \sum_{k=1}^{n} \frac{p(x)}{x - a_k}, \quad 即 \quad \frac{p'(x)}{p(x)} = \sum_{k=1}^{n} \frac{1}{x - a_k}.$$

再次求导得到:

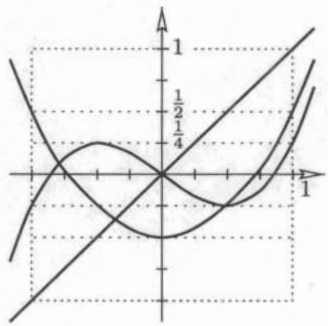
$$\frac{p''(x)p(x) - p'(x)^2}{p(x)^2} = -\sum_{k=1}^{n} \frac{1}{(x - a_k)^2} < 0. \qquad \square$$

附录: Chebyshev 定理

定理. 假设 $p(x)$ 是次数为 $n \geqslant 1$, 首项系数为 1 的实多项式, 那么

$$\max_{-1 \leqslant x \leqslant 1} |p(x)| \geqslant \frac{1}{2^{n-1}}.$$

在证明这个定理之前, 让我们先看看等式成立的一些例子. 边图描绘了次数为 1, 2 和 3 的使上述不等式等号成立的多项式的曲线, 事实上, 我们将要证明对于次数 n, 恰好存在一个使得 Chebyshev 定理中等式成立的多项式.



多项式 $p_1(x) = x$, $p_2(x) = x^2 - \frac{1}{2}$ 和 $p_3(x) = x^3 - \frac{3}{4}x$ 使 Chebyshev 定理中的等号成立.

■ **证明.** 考虑首项系数为 1 的实多项式 $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. 因为我们对 $-1 \leqslant x \leqslant 1$ 范围内的数感兴趣, 所以我们令 $x = \cos\vartheta$, $g(\vartheta) := p(\cos\vartheta)$, 故得到如下关于 $\cos\theta$ 的多项式:

$$g(\vartheta) = (\cos\vartheta)^n + a_{n-1}(\cos\vartheta)^{n-1} + \cdots + a_0. \qquad (1)$$

证明将按如下两步展开, 这两步本身也是非常经典和有趣的结果.

(A) 我们将 $g(\vartheta)$ 展成所谓的余弦多项式, 即具有如下形式的多项式:

$$g(\vartheta) = b_n \cos n\vartheta + b_{n-1}\cos(n-1)\vartheta + \cdots + b_1\cos\vartheta + b_0. \qquad (2)$$

我们要证明 $b_k \in \mathbb{R}$ 且 $b_n = \frac{1}{2^{n-1}}$.

(B) 给定任意 n 阶多项式 $h(\vartheta)$ (表示 λ_n 是最高阶非零系数)

$$h(\vartheta) = \lambda_n \cos n\vartheta + \lambda_{n-1}\cos(n-1)\vartheta + \cdots + \lambda_0, \qquad (3)$$

我们要证明 $|\lambda_n| \leqslant \max|h(\vartheta)|$, 且将该不等式运用于 $g(\vartheta)$ 我们将得到定理的证明.

(A) 的证明. 为了从 (1) 得到 (2), 我们必须将所有的 $(\cos\vartheta)^k$ 展成余弦多项式的形式. 例如, 根据余弦的加法定理我们得到如下等式:

$$\cos 2\vartheta \;=\; \cos^2\vartheta - \sin^2\vartheta \;=\; 2\cos^2\vartheta - 1,$$

因此 $\cos^2\vartheta = \frac{1}{2}\cos 2\vartheta + \frac{1}{2}$. 为了转化 $\cos\vartheta$ 的任意次幂 $(\cos\vartheta)^k$, 我们通过关系式 $e^{ix} = \cos x + i\sin x$ 来考虑复数. e^{ix} 是模为 1 的复数 (参看第 5章方框中有关复单位根的内容). 特别地, 这个表明

$$e^{in\vartheta} \;=\; \cos n\vartheta + i\sin n\vartheta. \tag{4}$$

另一方面,

$$e^{in\vartheta} \;=\; (e^{i\vartheta})^n \;=\; (\cos\vartheta + i\sin\vartheta)^n. \tag{5}$$

由 (4) 和 (5) 的实部相等, 并且 $i^{4\ell+2} = -1$, $i^{4\ell} = 1$ 以及 $\sin^2\theta = 1-\cos^2\theta$, 我们得到

$$\begin{aligned}\cos n\vartheta \;&=\; \sum_{\ell\geqslant 0}\binom{n}{4\ell}(\cos\vartheta)^{n-4\ell}(1-\cos^2\vartheta)^{2\ell}\\ &\quad -\sum_{\ell\geqslant 0}\binom{n}{4\ell+2}(\cos\vartheta)^{n-4\ell-2}(1-\cos^2\vartheta)^{2\ell+1}.\end{aligned} \tag{6}$$

我们得到结论: $\cos n\vartheta$ 是 $\cos\vartheta$ 的多项式,

$$\cos n\vartheta \;=\; c_n(\cos\vartheta)^n + c_{n-1}(\cos\vartheta)^{n-1} + \cdots + c_0. \tag{7}$$

从 (6) 我们得到最高次系数是:

$$c_n \;=\; \sum_{\ell\geqslant 0}\binom{n}{4\ell} + \sum_{\ell\geqslant 0}\binom{n}{4\ell+2} \;=\; 2^{n-1}.$$

对于任意 $n > 0$ 有 $\sum_{k\geqslant 0}\binom{n}{2k} = 2^{n-1}$ 成立: 在 "需要" 的时候我们在集合 $\{1,2,\cdots,n-1\}$ 中加入元素 n, 则集合 $\{1,2,\cdots,n-1\}$ 的每个子集可以产生一个基数为偶数的集合 $\{1,2,\cdots,n\}$ 中的子集.

现在我们回到我们的论述. 归纳地, 假设对于任意 $k < n$, $(\cos\vartheta)^k$ 可以表示成 k 次余弦多项式, 从 (7) 中我们可以得到 $(\cos\vartheta)^n$ 可以表示成首项系数为 $b_n = \frac{1}{2^{n-1}}$ 次数为 n 的余弦多项式.

(B) 的证明. 令 $h(\vartheta)$ 是 (3) 中次数为 n 的余弦多项式, 不失一般性我们假设 $\lambda_n > 0$. 现在我们令 $m(\vartheta) := \lambda_n \cos n\vartheta$ 且有下式成立

$$m(\tfrac{k}{n}\pi) \;=\; (-1)^k\lambda_n, \qquad \text{对于 } k = 0, 1, \cdots, n.$$

用反证法, 假设 $\max|h(\vartheta)| < \lambda_n$, 则

$$m(\tfrac{k}{n}\pi) - h(\tfrac{k}{n}\pi) \ = \ (-1)^k\lambda_n - h(\tfrac{k}{n}\pi)$$

在范围 $0 \leqslant k \leqslant n$ 内对任意偶数 k 是正的, 对任意奇数 k 是负的. 我们得到结论: $m(\vartheta) - h(\vartheta)$ 在区间 $[0,\pi]$ 中至少有 n 个根. 但是这是不可能的, 因为 $m(\vartheta) - h(\vartheta)$ 是 $n-1$ 次的余弦多项式, 故其至多只有 $n-1$ 个根.

因此 **(B)** 的证明完毕, 同样 Chebyshev 定理的证明也完成. □

现在读者可以很容易完成证明: 即 $g_n(\vartheta) := \frac{1}{2^{n-1}}\cos n\vartheta$ 是唯一一个首项系数为 1 且使得等式 $\max|g(\vartheta)| = \frac{1}{2^{n-1}}$ 成立的 n 次余弦多项式.

我们称多项式 $T_n(x) = \cos n\vartheta$, $x = \cos\vartheta$, 为 *Chebyshev* 多项式 (第一型的); 因此 $\frac{1}{2^{n-1}}T_n(x)$ 是唯一使得 Chebyshev 定理中等式成立的次数为 n 的首 1 多项式.

参考文献

[1] P. L. Cebycev: *Œuvres,* Vol. I, Acad. Imperiale des Sciences, St. Petersburg 1899, pp. 387-469.

[2] G. Pólya: *Beitrag zur Verallgemeinerung des Verzerrungssatzes auf mehrfach zusammenhängenden Gebieten,* Sitzungsber. Preuss. Akad. Wiss. Berlin (1928), 228-232; Collected Papers Vol. I, MIT Press 1974, 347-351.

[3] G. Pólya & G. Szegő: *Problems and Theorems in Analysis, Vol. II,* Springer-Verlag, Berlin Heidelberg New York 1976; Reprint 1998.

Littlewood 和 Offord 的一个引理

第 19 章

在 1943 年 Littlewood 和 Offord 在他们关于代数方程根分布的著作中, 证明了以下的结果:

令 $a_1, a_2, \cdots, a_n$ 为复数且对所有的 i, $|a_i| \geqslant 1$. 考虑 2^n 个线性组合: $\sum_{i=1}^{n} \varepsilon_i a_i$, 其中 $\varepsilon_i \in \{1, -1\}$. 则落在任意半径为 1 的圆内的和 $\sum_{i=1}^{n} \varepsilon_i a_i$ 的个数不超过

$$c \frac{2^n}{\sqrt{n}} \log n, \quad c > 0 \text{ 是某个常数.}$$



John E. Littlewood

几年后, Paul Erdős 证明了这个上界而且去掉了 $\log n$ 项. 更有意思的是, 他证明了这个结果事实上是 Sperner 定理的一个简单推论 (见第 23 章).

让我们看看所有的 a_i 都是实数的情形来找一点证明的感觉. 不妨设所有的 a_i 都是正的 (若 $a_i < 0$, 则把 a_i 换为 $-a_i$, 把 ε_i 换为 $-\varepsilon_i$). 现在设一些组合 $\sum \varepsilon_i a_i$ 落在某个长为 2 的区间里. 令 $N = \{1, 2, \cdots, n\}$ 表示指标集. 对每个 $\sum \varepsilon_i a_i$, 置 $I := \{i \in N : \varepsilon_i = 1\}$. 现在若对任意的两个这样的子集有 $I \subsetneqq I'$, 则

$$\sum \varepsilon_i' a_i - \sum \varepsilon_i a_i = 2 \sum_{i \in I' \setminus I} a_i \geqslant 2,$$

矛盾. 故这些集合 I 构成一个反链, 从而根据 Sperner 的定理至多有 $\binom{n}{\lfloor n/2 \rfloor}$ 多个线性组合. 由 Stirling 公式 (见第 2 章) 我们得到

$$\binom{n}{\lfloor n/2 \rfloor} \leqslant c \frac{2^n}{\sqrt{n}}, \quad \text{对某个} c > 0.$$

Sperner 定理. 每个由 n- 集合的子集组成的反链的基数至多是 $\binom{n}{\lfloor n/2 \rfloor}$.

当 n 是偶数且所有的 $a_i = 1$, 得到 $\binom{n}{n/2}$ 个线性组合 $\sum_{i=1}^{n} \varepsilon_i a_i$, 加起来都是 0. 单看区间 $(-1, 1)$ 我们就发现二项式系数给出了精确的上界.

Erdős 在同一篇文章里猜想 $\binom{n}{\lfloor n/2 \rfloor}$ 也是复数情形的上界 (他仅能对某个 c 证明 $c\,2^n n^{-1/2}$ 是可以的). 事实上在实 Hilbert 空间中, 对满足 $|\boldsymbol{a}_i| \geqslant 1$ 的向量 $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$, 这个界也是成立的, 此时半径为 1 圆被替换为半径为 1 的开球.

Erdős 是正确的, 但历时二十年方有 Gyula Katona 和 Daniel Kleitman 分别独立证明了复数的情形 (或者等同于说, 平面 $\mathbb{R}^2$ 的情况). 他们的证明显然用到了平面的二维性质, 所以还不清楚如何推广到有限维实向量空间.

但是接着在 1970 年 Kleitman 证明了关于 Hilbert 空间的整个猜想, 他的论证惊人地简洁. 事实上, 他证明的还要多. 他的论证是当你发现了正确的归纳假设时如何着手的一个最好的例子.

不熟悉 Hilbert 空间的概念的读者不用担心: 我们并不真的需要一般的 Hilbert 空间. 既然我们处理的不过是有限多个向量 $\boldsymbol{a}_i$, 考虑具有普通内积的实空间 $\mathbb{R}^d$ 也就够了. 下面就是 Kleitman 的结果.

> **定理.** 令 $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ 为 $\mathbb{R}^d$ 中长度至少为 1 的向量, $R_1, \cdots, R_k$ 是 $\mathbb{R}^d$ 中的 k 个开区域且每个 R_i 的直径度不大于 2. 那么在这些区域的并 $\bigcup_i R_i$ 中的线性组合 $\sum_{i=1}^n \varepsilon_i \boldsymbol{a}_i, \varepsilon_i \in \{1, -1\}$ 的个数, 至多是 k 个最大的二项式系数 $\binom{n}{j}$ 的和. 特别地, 当 $k = 1$, 就得到界 $\binom{n}{\lfloor n/2 \rfloor}$.

证明之前注意到这个界对下面的向量组是精确的:

$$\boldsymbol{a}_1 = \cdots = \boldsymbol{a}_n = \boldsymbol{a} = (1, 0, \cdots, 0)^T.$$

事实上, 若 n 是偶数, 有 $\binom{n}{n/2}$ 个和加起来是 $\overrightarrow{0}$, $\binom{n}{n/2-1}$ 个和加起来是 $(-2)\boldsymbol{a}$, $\binom{n}{n/2+1}$ 个和加起来是 $2\boldsymbol{a}$, 等等. 选择半径为 1 的球, 中心分别是

$$-2\lceil \tfrac{k-1}{2} \rceil \boldsymbol{a}, \quad \cdots, \quad (-2)\boldsymbol{a}, \quad \mathbf{0}, \quad 2\boldsymbol{a}, \quad \cdots, \quad 2\lfloor \tfrac{k-1}{2} \rfloor \boldsymbol{a},$$

得到

$$\binom{n}{\lfloor \frac{n-k+1}{2} \rfloor} + \cdots + \binom{n}{\frac{n-2}{2}} + \binom{n}{\frac{n}{2}} + \binom{n}{\frac{n+2}{2}} + \cdots + \binom{n}{\lfloor \frac{n+k-1}{2} \rfloor}$$

之和在这 k 个球里面. 由于最大二项式系数从中心向两端分布, 这正是我们承诺证明的表示 (参见第 2 章). 当 n 为奇数推理是类似的.

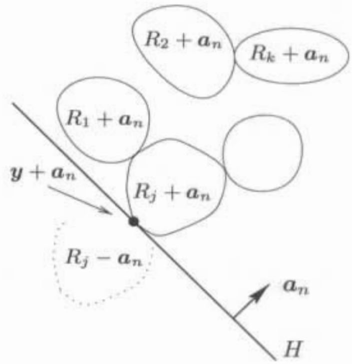
■ **证明.** 不失一般性, 从现在开始假设 R_i 互不相交. 证明的关键是二项式系数的一个递推式, 它告诉我们怎样把关于 n 的和关于 $n-1$ 的最大二项式系数联系起来. 置 $r = \lfloor \frac{n-k+1}{2} \rfloor$, $s = \lfloor \frac{n+k-1}{2} \rfloor$, 则 $\binom{n}{r}, \binom{n}{r+1}, \cdots, \binom{n}{s}$ 是关于 n 的 k 个最大的二项式系数. 递推关系 $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$ 表明

$$\begin{aligned}\sum_{i=r}^{s}\binom{n}{i} &= \sum_{i=r}^{s}\binom{n-1}{i}+\sum_{i=r}^{s}\binom{n-1}{i-1}\\ &= \sum_{i=r}^{s}\binom{n-1}{i}+\sum_{i=r-1}^{s-1}\binom{n-1}{i} \qquad (1)\\ &= \sum_{i=r-1}^{s}\binom{n-1}{i}+\sum_{i=r}^{s-1}\binom{n-1}{i},\end{aligned}$$

易见第一个和是把形如 $\binom{n-1}{i}$ 的 $k+1$ 个最大的二项式系数加起来, 第二个和是把 $k-1$ 个最大的项加起来.

Kleitman 的证明是对 n 归纳: $n=1$ 显然. 鉴于 (1), 我们只需证明分布在 k 个不交区域的线性组合 $\boldsymbol{a}_1,\cdots,\boldsymbol{a}_n$ 可以通过一个双射与分布在 $k+1$ 个区域的或 $k-1$ 个区域的线性组合 $\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{n-1}$ 对应起来.

断言. 至少存在一个平移以后的区域 $R_j-\boldsymbol{a}_n$ 与平移后的区域 $R_1+\boldsymbol{a}_n,\cdots,R_k+\boldsymbol{a}_n$ 都不交.



欲证明断言, 考虑这样一个与 $\boldsymbol{a}_n$ 垂直的超平面 $H=\{\boldsymbol{x}:\langle\boldsymbol{a}_n,\boldsymbol{x}\rangle=c\}$: 所有平移了的区域 $R_i+\boldsymbol{a}_n$ 都在它的同一侧 $\langle\boldsymbol{a}_n,\boldsymbol{x}\rangle\geqslant c$, 并且其与某个平移了的区域的闭包接触, 不妨设为 $R_j+\boldsymbol{a}_n$. 因为每个区域都有界, 这样的超平面是存在的. 由 R_j 是开的, 对任意的 $\boldsymbol{x}\in R_j$ 以及 R_j 边界上的 $\boldsymbol{y}$, 有 $|\boldsymbol{x}-\boldsymbol{y}|<2$. 往证 $R_j-\boldsymbol{a}_n$ 在 H 的另一边. 假设不然, 存在某个 $\boldsymbol{x}\in R_j$ 使得 $\langle\boldsymbol{a}_n,\boldsymbol{x}-\boldsymbol{a}_n\rangle\geqslant c$, 亦即$\langle\boldsymbol{a}_n,\boldsymbol{x}\rangle\geqslant|\boldsymbol{a}_n|^2+c$.

令 $\boldsymbol{y}+\boldsymbol{a}_n$ 为 H 接触 $R_j+\boldsymbol{a}_n$ 处的一点, 即 $\boldsymbol{y}$ 在 R_j 的边界上, 有 $\langle\boldsymbol{a}_n,\boldsymbol{y}+\boldsymbol{a}_n\rangle=c$, 换言之 $\langle\boldsymbol{a}_n,-\boldsymbol{y}\rangle=|\boldsymbol{a}_n|^2-c$, 则

$$\langle\boldsymbol{a}_n,\boldsymbol{x}-\boldsymbol{y}\rangle\geqslant 2|\boldsymbol{a}_n|^2.$$

从 Cauchy-Schwarz 不等式推得

$$2|\boldsymbol{a}_n|^2\leqslant\langle\boldsymbol{a}_n,\boldsymbol{x}-\boldsymbol{y}\rangle\leqslant|\boldsymbol{a}_n||\boldsymbol{x}-\boldsymbol{y}|,$$

于是 (由 $|\boldsymbol{a}_n|\geqslant 1$) 得到 $2\leqslant 2|\boldsymbol{a}_n|\leqslant|\boldsymbol{x}-\boldsymbol{y}|$, 矛盾.

剩下的就容易了. 将位于$R_1\cup\cdots\cup R_k$的组合 $\sum\varepsilon_i\boldsymbol{a}_i$ 分为两类: 把所有满足 $\varepsilon_n=-1$, 或 $\varepsilon_n=1$ 同时位于 R_j 的 $\sum_{i=1}^{n}\varepsilon_i\boldsymbol{a}_i$ 放在第一类; 把剩余的组合, 即满足 $\varepsilon_n=1$ 并且在 R_j 之外的 $\sum_{i=1}^{n}\varepsilon_i\boldsymbol{a}_i$ 放在第二类. 于是与第一类对应的组合 $\sum_{i=1}^{n-1}\varepsilon_i\boldsymbol{a}_i$ 位于 $k+1$ 个不交区域 $R_1+\boldsymbol{a}_n,\cdots,R_k+\boldsymbol{a}_n$ 及 $R_j-\boldsymbol{a}_n$, 与第二类对应的组合 $\sum_{i=1}^{n-1}\varepsilon_i\boldsymbol{a}_i$ 位于$k-1$个不交区域 $R_1-\boldsymbol{a}_n,\cdots,R_k-\boldsymbol{a}_n$ (缺 $R_j-\boldsymbol{a}_n$). 由归纳假设,

第一类含至多 $\sum_{i=r-1}^{s}\binom{n-1}{i}$ 个组合, 而第二类含至多 $\sum_{i=r}^{s-1}\binom{n-1}{i}$ 个组合, 再由 (1) 就完成了整个证明, 纯粹的天书证明. □

参考文献

[1] P. Erdős: *On a lemma of Littlewood and Offord,* Bulletin. Amer. Math. Soc. **51** (1945), 898-902.

[2] G. Katona: *On a conjecture of Erdős and a stronger form of Sperner's theorem,* Studia Sci. Math. Hungar. **1** (1966), 59-63.

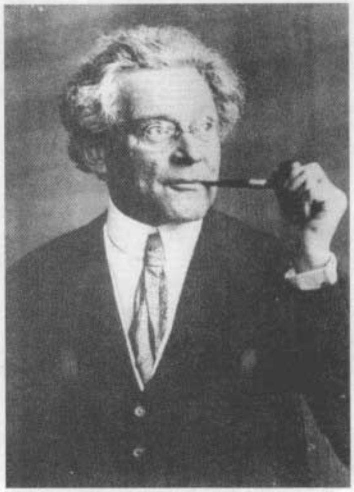
[3] D. Kleitman: *On a lemma of Littlewood and Offord on the distribution of certain sums,* Math. Zeitschrift. **90** (1965), 251-259.

[4] D. Kleitman: *On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors,* Advances Math. **5** (1970), 155-157.

[5] J. E. Littlewood & A. C. Offord: *On the number of real roots of a random algebraic equation III,* Mat. USSR Sb. **12** (1943), 277-285.

余切与 Herglotz 技巧

第 20 章



Gustav Herglotz

涉及初等函数的公式哪个最有趣? Jürgen Elstrodt 在他的优美文章 [2] 里 (以下仿效其叙述) 首推余切函数的部分分式展开:

$$\pi \cot \pi x \;=\; \frac{1}{x} + \sum_{n=1}^{\infty} \Big(\frac{1}{x+n} + \frac{1}{x-n}\Big) \qquad (x \in \mathbb{R}\backslash\mathbb{Z}).$$

这个优雅的公式是 Euler 于 1748 年在他的著作 *Introductio in Analysin Infinitorum* 的 §178 中证明的, 这可算作他的最佳成就之一. 我们还可将之写得更优美

$$\pi \cot \pi x = \lim_{N\to\infty} \sum_{n=-N}^{N} \frac{1}{x+n}. \tag{1}$$

但须谨慎, 求和 $\sum_{n\in\mathbb{Z}} \frac{1}{x+n}$ 有点危险: 因为这个和只是条件收敛的, 所以其值依赖于 "正确的" 求和顺序.

我们将要用惊人的简洁方式推导出 (1), 这归功于 Gustav Herglotz 的 "Herglotz 技巧". 作为开始, 置

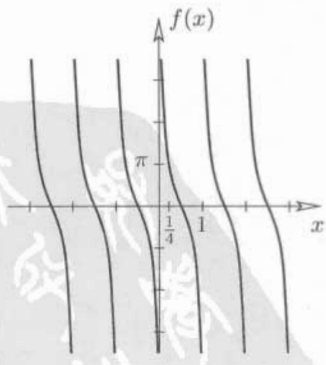
$$f(x) \;:=\; \pi \cot \pi x, \qquad g(x) \;:=\; \lim_{N\to\infty} \sum_{n=-N}^{N} \frac{1}{x+n}.$$

让我们试推出这两个函数足够多的共同性质, 最终看出它们必是同一个……

(A) 函数 f 与 g 在所有非整数值处有定义, 且连续.

显而易见对余切函数 $f(x) = \pi \cot \pi x = \pi \frac{\cos \pi x}{\sin \pi x}$ 这是对的 (见图). 对 $g(x)$, 先用 $\frac{1}{x+n} + \frac{1}{x-n} = -\frac{2x}{n^2-x^2}$ 将 Euler 的公式改写为

$$\pi \cot \pi x = \frac{1}{x} - \sum_{n=1}^{\infty} \frac{2x}{n^2-x^2}. \tag{2}$$



函数 $f(x) = \pi \cot \pi x$

于是关于**(A)** 须证对每个 $x \notin \mathbb{Z}$,

$$\sum_{n=1}^{\infty} \frac{1}{n^2-x^2}$$

在 x 的某个邻域一致收敛.

为此, 无需考虑第一项, 即当 $n=1$, 或者任何使得 $2n-1 \leqslant x^2$ 的项, 因为只有有限多个这样的项. 另一方面, 当 $n \geqslant 2$ 及 $2n-1 > x^2$, 亦即 $n^2 - x^2 > (n-1)^2 > 0$, 这些项有界

$$0 \ < \ \frac{1}{n^2 - x^2} \ < \ \frac{1}{(n-1)^2}.$$

以上的界不仅对 x 本身成立, 还对 x 的某个邻域中的值都对. 最后 $\sum \frac{1}{(n-1)^2}$ 收敛 (到 $\frac{\pi^2}{6}$, 见第 7 章) 这个事实提供了证明 **(A)**所需的一致收敛性.

(B) f 与 g 都是以 1 为周期 的函数, 亦即 $f(x+1) = f(x)$ 与 $g(x+1) = g(x)$ 对所有的 $x \in \mathbb{R}\backslash\mathbb{Z}$ 成立.

由余切函数的周期是 π, f 的周期是 1 (再看上图). 对 g 我们如下论证. 置

$$g_N(x) \ := \ \sum_{n=-N}^{N} \frac{1}{x+n},$$

则

$$\begin{aligned} g_N(x+1) \ &= \ \sum_{n=-N}^{N} \frac{1}{x+1+n} \ = \ \sum_{n=-N+1}^{N+1} \frac{1}{x+n} \\ &= \ g_{N-1}(x) + \frac{1}{x+N} + \frac{1}{x+N+1}. \end{aligned}$$

从而

$$g(x+1) = \lim_{N\to\infty} g_N(x+1) = \lim_{N\to\infty} g_{N-1}(x) = g(x).$$

(C) f 与 g 都是奇函数, 亦即有 $f(-x) = -f(x)$ 与 $g(-x) = -g(x)$ 对所有的 $x \in \mathbb{R}\backslash\mathbb{Z}$ 成立.

函数 f 显然有这个性质, 对 g 则只须观察到 $g_N(-x) = -g_N(x)$.

最后的两个事实构成了 Herglotz 技巧: 首先证明 f 和 g 满足同一个函数方程, 其次 $h := f - g$ 可以连续地延伸到整个 $\mathbb{R}$ 上.

(D) 函数 f 与 g 满足相同的函数方程:

$$f(\frac{x}{2}) + f(\frac{x+1}{2}) = 2f(x).$$

对 $f(x)$ 这个结果来自正弦和余弦函数的和角定理:

$$f(\tfrac{x}{2}) + f(\tfrac{x+1}{2}) = \pi\left[\frac{\cos\frac{\pi x}{2}}{\sin\frac{\pi x}{2}} - \frac{\sin\frac{\pi x}{2}}{\cos\frac{\pi x}{2}}\right]$$

$$= 2\pi\frac{\cos(\frac{\pi x}{2}+\frac{\pi x}{2})}{\sin(\frac{\pi x}{2}+\frac{\pi x}{2})} = 2\,f(x).$$

和角定理:

$\sin(x+y) = \sin x\cos y + \cos x\sin y$

$\cos(x+y) = \cos x\cos y - \sin x\sin y$

$\Longrightarrow \sin(x+\frac{\pi}{2}) = \cos x$

$\cos(x+\frac{\pi}{2}) = -\sin x$

$\sin x = 2\sin\frac{x}{2}\cos\frac{x}{2}$

$\cos x = \cos^2\frac{x}{2} - \sin^2\frac{x}{2}.$

g 的函数方程来自

$$g_N(\tfrac{x}{2}) + g_N(\tfrac{x+1}{2}) = 2\,g_{2N}(x) + \frac{2}{x+2N+1},$$

上式则是因为

$$\frac{1}{\frac{x}{2}+n} + \frac{1}{\frac{x+1}{2}+n} = 2\Big(\frac{1}{x+2n} + \frac{1}{x+2n+1}\Big).$$

现在看

$$h(x) = f(x) - g(x) = \pi\cot\pi x - \Big(\frac{1}{x} - \sum_{n=1}^{\infty}\frac{2x}{n^2-x^2}\Big). \qquad (3)$$

我们已经知道 h 是 $\mathbb{R}\backslash\mathbb{Z}$ 上的连续函数, 且满足性质**(B)**, **(C)** 和**(D)**. 在整数点如何呢? 从正弦和余弦函数的级数展开, 或应用 de l'Hospital 法则两次, 我们发现

$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} \pm \cdots$

$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} \pm \cdots$

$$\lim_{x\to 0}\Big(\cot x - \frac{1}{x}\Big) = \lim_{x\to 0}\frac{x\cos x - \sin x}{x\sin x} = 0,$$

从而也有

$$\lim_{x\to 0}\Big(\pi\cot\pi x - \frac{1}{x}\Big) = 0.$$

但由于 (3) 中的最后一个和式 $\sum_{n=1}^{\infty}\frac{2x}{n^2-x^2}$ 当 $x \longrightarrow 0$ 时收敛到 0, 我们实际有 $\lim\limits_{x\to 0}h(x) = 0$, 从而由周期性

$$\lim_{x\to n}h(x) = 0, \qquad \text{对所有} n\in\mathbb{Z}.$$

总结一下, 我们证明了

(E)　对 $x\in\mathbb{Z}$, 置 $h(x) := 0$, 则 h 成为整个 $\mathbb{R}$ 上的连续函数, 且满足性质**(B)**, **(C)** 和 **(D)**.

我们已为最后一击准备就绪. 既然 h 是连续的周期性函数, 它就有个最大值 m. 令 x_0 为 $[0,1]$ 中取得最大值 $h(x_0) = m$ 的点. 由**(D)**, 有

$$h(\tfrac{x_0}{2}) + h(\tfrac{x_0+1}{2}) = 2m,$$

于是 $h(\frac{x_0}{2}) = m$. 重复之得到 $h(\frac{x_0}{2^n}) = m$ 对所有的 n 成立, 从而由连续性 $h(0) = m$. 而 $h(0) = 0$, 故 $m = 0$, 换言之对所有的 $x \in \mathbb{R}$, 有 $h(x) \leqslant 0$. 因为 $h(x)$ 是奇函数, 就不可能存在 $h(x) < 0$, 从而对所有的 $x \in \mathbb{R}$, 有 $h(x) = 0$. Euler 的定理证毕. □

可以从 (1) 得到很多推论, 最著名的一个是关于 Riemann zeta 函数在正偶数处取值的问题 (见第 6 章的附录):

$$\zeta(2k) \;=\; \sum_{n=1}^{\infty} \frac{1}{n^{2k}} \qquad (k \in \mathbb{N}). \tag{4}$$

那么让我们看看 Euler 在几年后的 1755 年是怎样处理级数 (4) 的, 以结束我们这章. 从公式 (2) 开始. 在 (2) 两端同乘 x, 再令 $y = \pi x$, 我们发现当 $|y| < \pi$:

$$\begin{aligned} y \cot y \;&=\; 1 - 2\sum_{n=1}^{\infty} \frac{y^2}{\pi^2 n^2 - y^2} \\ &=\; 1 - 2\sum_{n=1}^{\infty} \frac{y^2}{\pi^2 n^2} \frac{1}{1 - \left(\frac{y}{\pi n}\right)^2}. \end{aligned}$$

最后一个因式是几何级数的和, 所以

$$\begin{aligned} y \cot y \;&=\; 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \left(\frac{y}{\pi n}\right)^{2k} \\ &=\; 1 - 2\sum_{k=1}^{\infty} \Big(\frac{1}{\pi^{2k}} \sum_{n=1}^{\infty} \frac{1}{n^{2k}}\Big) y^{2k}. \end{aligned}$$

于是我们证明了这个值得注意的结果:

对所有的 $k \in \mathbb{N}$, 项 y^{2k} 在 $y \cot y$ 的幂级数展开中的系数等于

$$[y^{2k}]\, y \cot y \;=\; -\frac{2}{\pi^{2k}} \sum_{n=1}^{\infty} \frac{1}{n^{2k}} \;=\; -\frac{2}{\pi^{2k}} \zeta(2k). \tag{5}$$

另有一种也许 "典型" 得多的方法来得到 $y \cot y$ 的级数展开. 从分析中我们知道 $e^{iy} = \cos y + i \sin y$, 从而

$$\cos y \;=\; \frac{e^{iy} + e^{-iy}}{2}, \qquad \sin y \;=\; \frac{e^{iy} - e^{-iy}}{2i},$$

表明

$$y \cot y \;=\; iy \frac{e^{iy} + e^{-iy}}{e^{iy} - e^{-iy}} \;=\; iy \frac{e^{2iy} + 1}{e^{2iy} - 1}\,.$$

作替换 $z = 2iy$, 得

$$y\cot y \;=\; \frac{z}{2}\,\frac{e^z+1}{e^z-1} \;=\; \frac{z}{2} + \frac{z}{e^z-1}\,. \tag{6}$$

因此我们所需要的是函数 $\frac{z}{e^z-1}$ 的幂级数展开; 注意这个函数是定义在整个 $\mathbb{R}$ 上并且连续的 (对 $z=0$ 利用指数函数的幂级数, 或者 de l'Hospital 法则可得结果为 1). 记

$$\frac{z}{e^z-1} \;=:\; \sum_{n\geqslant 0} B_n \frac{z^n}{n!}\,. \tag{7}$$

系数 B_n 被称为 *Bernoulli 数*. (6) 的左端是偶函数 (亦即 $f(z)=f(-z)$), 故知对奇的 $n \geqslant 3$ 有 $B_n = 0$, 而 $B_1 = -\frac{1}{2}$ 对应 (6) 中的 $\frac{z}{2}$.

由

$$\Big(\sum_{n\geqslant 0} B_n \frac{z^n}{n!}\Big)(e^z-1) \;=\; \Big(\sum_{n\geqslant 0} B_n \frac{z^n}{n!}\Big)\Big(\sum_{n\geqslant 1} \frac{z^n}{n!}\Big) \;=\; z,$$

通过比较 z^n 的系数得:

$$\sum_{k=0}^{n-1} \frac{B_k}{k!(n-k)!} = \begin{cases} 1 & 当\, n=1, \\ 0 & 当\, n\neq 1. \end{cases} \tag{8}$$

n	0	1	2	3	4	5	6	7	8
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$

前几个 Bernoulli 数

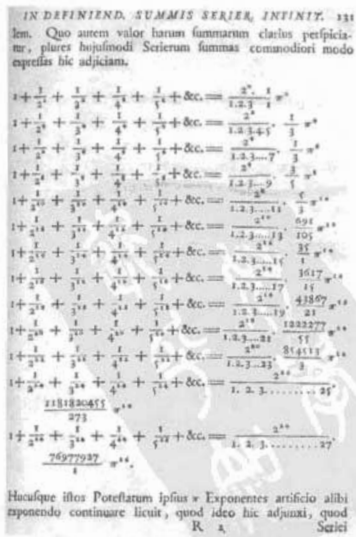
可以从 (8) 递归地计算 Bernoulli 数. 当 $n=1$ 有 $B_0 = 1$, 当 $n=2$ 有 $\frac{B_0}{2} + B_1 = 0$, 亦即 $B_1 = -\frac{1}{2}$, 以此类推.

现在我们几乎大功告成: 结合 (6) 与 (7) 即得

$$y\cot y \;=\; \sum_{k=0}^{\infty} B_{2k}\frac{(2iy)^{2k}}{(2k)!} \;=\; \sum_{k=0}^{\infty} \frac{(-1)^k 2^{2k} B_{2k}}{(2k)!} y^{2k},$$

再由 (5), 就有关于 $\zeta(2k)$ 的 Euler 公式:

$$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} \;=\; \frac{(-1)^{k-1}2^{2k-1}B_{2k}}{(2k)!}\,\pi^{2k} \qquad (k\in\mathbb{N}). \tag{9}$$


IN DEFINIEND. SUMMIS SERIER. INFINIT. 131

lem. Quo autem valor harum fummarum clarius perfpiciatur, plures hujufmodi Serierum fummas commodiori modo expreffas hic adjiciam.

$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\&c. = \frac{2^0}{1.2.3}\cdot\frac{1}{1}\pi^2$

$1+\frac{1}{2^4}+\frac{1}{3^4}+\frac{1}{4^4}+\frac{1}{5^4}+\&c. = \frac{2^2}{1.2.3.4.5}\cdot\frac{1}{3}\pi^4$

$1+\frac{1}{2^6}+\frac{1}{3^6}+\frac{1}{4^6}+\frac{1}{5^6}+\&c. = \frac{2^4}{1.2.3\ldots7}\cdot\frac{1}{3}\pi^6$

$1+\frac{1}{2^8}+\frac{1}{3^8}+\frac{1}{4^8}+\frac{1}{5^8}+\&c. = \frac{2^6}{1.2.3\ldots9}\cdot\frac{3}{5}\pi^8$

$1+\frac{1}{2^{10}}+\frac{1}{3^{10}}+\frac{1}{4^{10}}+\frac{1}{5^{10}}+\&c. = \frac{2^8}{1.2.3\ldots11}\cdot\frac{5}{3}\pi^{10}$

$1+\frac{1}{2^{12}}+\frac{1}{3^{12}}+\frac{1}{4^{12}}+\frac{1}{5^{12}}+\&c. = \frac{2^{10}}{1.2.3\ldots13}\cdot\frac{691}{105}\pi^{12}$

$1+\frac{1}{2^{14}}+\frac{1}{3^{14}}+\frac{1}{4^{14}}+\frac{1}{5^{14}}+\&c. = \frac{2^{12}}{1.2.3\ldots15}\cdot\frac{35}{1}\pi^{14}$

$1+\frac{1}{2^{16}}+\frac{1}{3^{16}}+\frac{1}{4^{16}}+\frac{1}{5^{16}}+\&c. = \frac{2^{14}}{1.2.3\ldots17}\cdot\frac{3617}{15}\pi^{16}$

$1+\frac{1}{2^{18}}+\frac{1}{3^{18}}+\frac{1}{4^{18}}+\frac{1}{5^{18}}+\&c. = \frac{2^{16}}{1.2.3\ldots19}\cdot\frac{43867}{21}\pi^{18}$

$1+\frac{1}{2^{20}}+\frac{1}{3^{20}}+\frac{1}{4^{20}}+\frac{1}{5^{20}}+\&c. = \frac{2^{18}}{1.2.3\ldots21}\cdot\frac{1222277}{55}\pi^{20}$

$1+\frac{1}{2^{22}}+\frac{1}{3^{22}}+\frac{1}{4^{22}}+\frac{1}{5^{22}}+\&c. = \frac{2^{20}}{1.2.3\ldots23}\cdot\frac{854513}{3}\pi^{22}$

$1+\frac{1}{2^{24}}+\frac{1}{3^{24}}+\frac{1}{4^{24}}+\frac{1}{5^{24}}+\&c. = \frac{2^{22}}{1.2.3\ldots\ldots25}\cdot\frac{1181820455}{273}\pi^{24}$

$1+\frac{1}{2^{26}}+\frac{1}{3^{26}}+\frac{1}{4^{26}}+\frac{1}{5^{26}}+\&c. = \frac{2^{24}}{1.2.3\ldots\ldots27}\cdot\frac{76977927}{1}\pi^{26}.$

Hucufque iftos Poteftatum ipfius π Exponentes artificio alibi exponendo continuare licuit, quod ideo hic adjunxi, quod

R 2　Seriei

1748 年 Euler 的著作《Introductio in Analysin Infinitorum》的第 131 页

读我们的 Bernoulli 数的表, 则再次得到第 7 章的和式 $\sum\frac{1}{n^2} = \frac{\pi^2}{6}$, 进而

$$\sum_{n=1}^{\infty}\frac{1}{n^4} = \frac{\pi^4}{90}, \qquad \sum_{n=1}^{\infty}\frac{1}{n^6} = \frac{\pi^6}{945}, \qquad \sum_{n=1}^{\infty}\frac{1}{n^8} = \frac{\pi^8}{9450},$$

$$\sum_{n=1}^{\infty}\frac{1}{n^{10}} = \frac{\pi^{10}}{93555}, \qquad \sum_{n=1}^{\infty}\frac{1}{n^{12}} = \frac{691\,\pi^{12}}{638512875}, \qquad \cdots$$

$\zeta(10)$ 的 Bernoulli 数 $B_{10}=\frac{5}{66}$ 看上去还好, 但是下一个 $\zeta(12)$ 需要的值 $B_{12}=-\frac{691}{2730}$ 就在分子上有了一个大素数因子 691. Euler 首先计算了 $\zeta(2k)$ 的几个值, 而未注意到与 Bernoulli 数的关联, 是这个奇怪的素数 691 的出现提醒了他.

意外的是, 既然当 $k\longrightarrow\infty$, $\zeta(2k)$ 收敛到 1, 方程 (9) 告诉我们数列 $|B_{2k}|$ 应该增长很快 —— 这从前几个值里是看不出来的.

对比之下, 我们对 Riemann zeta 函数在奇数点 $k\geqslant 3$ 的值所知甚少; 见第 7 章.

参考文献

[1] S. Bochner: *Book review of "Gesammelte Schriften" by Gustav Herglotz,* Bulletin. Amer. Math. Soc. **1** (1979), 1020-1022.

[2] J. Elstrodt: *Partialbruchzerlegung des Kotangens, Herglotz-Trick und die Weierstraßsche stetige, nirgends differenzierbare Funktion,* Math. Semesterberichte **45** (1998), 207-220.

[3] L. Euler: *Introductio in Analysin Infinitorum,* Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8. In English: *Introduction to Analysis of the Infinite,* Book I (translated by J. D. Blanton), Springer-Verlag, New York 1988.

[4] L. Euler: *Institutiones calculi differentialis cum ejus usu in analysi finitorum ac doctrina serierum,* Petersburg 1755; Opera Omnia, Ser. 1, Vol. 10.

Buffon 的投针问题 第 21 章

1777 年, 一位名叫 Georges Louis Leclerc (也就是 Comte de Buffon) 的法国贵族提出了下面的问题:

> 若将一根短针掷在一张有均匀横纹的纸上, 那么针落的位置与横线相交的概率是多大?



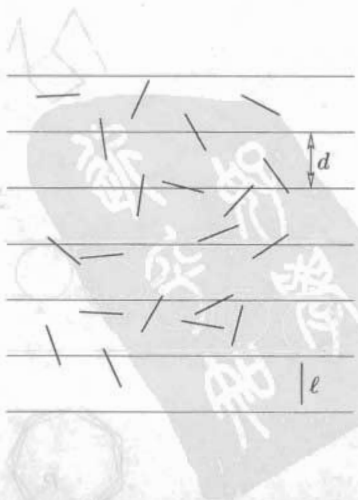
Le Comte de Buffon

这个概率依赖于横纹纸上横线间的距离 d, 也依赖于落针的长度 ℓ, 或者说由比率 $\frac{\ell}{d}$ 决定. 我们希望考虑的是短针, 其长度满足 $\ell \leqslant d$. 或者说, 短针不会同时交上两条横线 (同时以零的概率接触两根横线). Buffon 问题的答案也许令人惊讶: 里面包括了数 π.

定理 ("Buffon 的投针问题")

若一根长度为 ℓ 的短针, 抛在横线间距离为 $d \geqslant \ell$ 的均匀横纹纸上, 则针落在一个与某条横线相交的位置的概率恰为

$$p = \frac{2}{\pi}\frac{\ell}{d}.$$



这个结果意味着可以通过实验得到 π 的近似值: 掷针 N 次, 得到正面的结果 (相交) P 次, 则 $\frac{P}{N}$ 应大约是 $\frac{2}{\pi}\frac{\ell}{d}$, 亦即 π 可以由 $\frac{2\ell N}{dP}$ 逼近. 最大规模 (和最彻底的) 实验也许是 1901 年由 Lazzarini 完成的, 他甚至造了一个机器来把一根木棍抛掷 3408 次 (其 $\frac{\ell}{d} = \frac{5}{6}$). 和横线相交的次数是 1808 次, 从而得到近似 $\pi \approx 2 \cdot \frac{5}{6}\frac{3408}{1808} = 3.1415929....$ 这精确到 π 的第六位小数, 足够好了! (Lazzarini 选取的值直接联系到广为人知的近似 $\pi \approx \frac{355}{113}$; 见第 6 章. 这可以解释 3408 和 $\frac{5}{6}$, 要知道 $\frac{5}{6} \cdot 3408$ 是 355 的倍数. 更多关于 Lazzarini 的把戏参见 [5].)

投针问题可以通过计算定积分获得解决. 下面我们会那么做, 用这种方法还可以解决长针的问题. 但是 1860 年由 E. Barbier 发现的天书证明是不需要积分的, 它只要再丢一根不同的针 ……

抛一根任意的针, 可长可短, 则产生的交点数的数学期望是

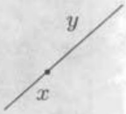
$$E = p_1 + 2p_2 + 3p_3 + \cdots,$$

其中 p_1 是针落下后刚好有 1 个交点的概率, p_2 是刚好有 2 个交点的概率, p_3 是刚好有 3 个交点的概率, 等等. Buffon 所问的是得到至少一个交点的概率

$$p \;=\; p_1 + p_2 + p_3 + \cdots.$$

(针恰好落在某横线之上的事件, 以及一个端点在某横线上的事件的概率都是 0, 所以在我们的讨论中将它们忽略不计.)

另一方面, 如果针是短的, 则得到多于一个交点的概率为零, $p_2 = p_3 = \cdots = 0$, 故有 $E = p$: 所求的概率正是交点数的期望. 如此表述极为重要, 因为我们就可以用到期望的线性性(参见第 14 章)了. 事实上, 记抛掷一根长为 ℓ 的针所产生的交点数的期望为 $E(\ell)$. 若 $\ell = x + y$, 则可考虑长为 x 的"前端"与长为 y 的"后端", 得



$$E(x+y) \;=\; E(x) + E(y).$$

因为交点数总是恰好等于前端产生的那些加上后端产生的那些.

在这个"函数方程"上对 n 归纳表明, 对所有的 $n \in \mathbb{N}$ 有 $E(nx) = nE(x)$, 进而

$$mE(\frac{n}{m}x) = E(m\frac{n}{m}x) = E(nx) = nE(x),$$

故 $E(rx) = rE(x)$ 对所有的有理数 $r \in \mathbb{Q}$ 成立. 此外, $E(x)$ 显然在 $x \geqslant 0$ 内单调, 从而在 $x \geqslant 0$ 内有 $E(x) = cx$, 其中 $c = E(1)$ 是某个常数. 那这个常数是什么呢?

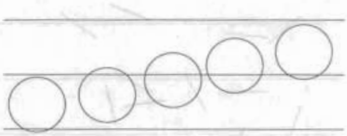


为此我们用一些不同形状的针. 事实上, 让我们抛一根"多边形"的针: 它包含几个直线段, 总长度也是 ℓ. 那么其产生的交点数 (以 1 的概率) 就是各个直线段产生的交点数之和. 所以, 由期望的线性性交点数的期望再次有



$$E \;=\; c\ell.$$

(直线段的组合方式规则或者不规则并不重要!)



Barbier 解决 Buffon 投针问题的关键是考察了一根直径为 d, 即长度为 $x = d\pi$ 的圆形针 C. 这样一根针如果掷到横纹纸上会产生刚好两个交点, 总是如此!

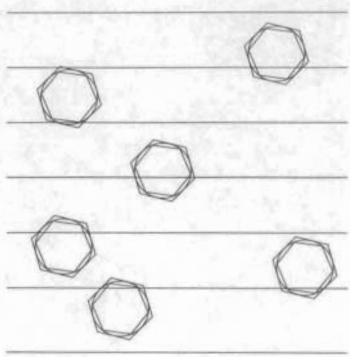


这个圆可以由多边形逼近. 想象一下, 在抛圆针 C 的同时我们抛一个内接的多边形针 P_n, 以及一个外切的多边形针 P^n. 每条与 P_n 相交的横线也必与 C 相交, 同时若横线与 C 相交也必与 P^n 相交. 因此, 交点数的期望满足

$$E(P_n) \leqslant E(C) \leqslant E(P^n).$$

现在 P_n 和 P^n 都是多边形, 故两者交点数的期望都是 "c 倍的长度", 对 C 的期望则是 2, 代回上式得到

$$c\,\ell(P_n) \leqslant 2 \leqslant c\,\ell(P^n). \qquad (1)$$



当 $n \longrightarrow \infty$, P_n 与 P^n 都逼近 C. 特别地,

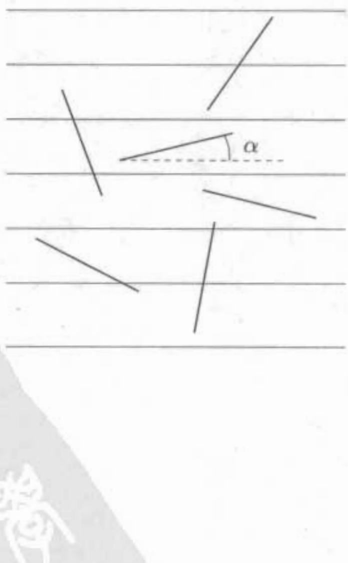
$$\lim_{n\to\infty} \ell(P_n) = d\pi = \lim_{n\to\infty} \ell(P^n).$$

于是当 $n \longrightarrow \infty$, 由 (1) 得

$$c\,d\pi \leqslant 2 \leqslant c\,d\pi,$$

从而 $c = \frac{2}{\pi}\frac{1}{d}$. □

但我们也可以用微积分证明! 得到一个 "简单" 积分的关键是考虑针的斜率; 不妨设其落在与水平线成 α 角的位置, 且 α 的取值范围是 $0 \leqslant \alpha \leqslant \frac{\pi}{2}$. (由对称性不计斜率为负的情形, 因为它与正斜率时概率相等.) 落在斜率为 α 处的针高度为 $\ell \sin\alpha$, 与间距为 d 的横线相交的概率是 $\frac{\ell \sin\alpha}{d}$. 于是对可能的角度 α 取平均值, 就得到概率



$$p = \frac{2}{\pi}\int_0^{\pi/2} \frac{\ell \sin\alpha}{d}\, d\alpha = \frac{2}{\pi}\frac{\ell}{d}\big[-\cos\alpha\big]_0^{\pi/2} = \frac{2}{\pi}\frac{\ell}{d}.$$

如果是长针, 只要 $\ell \sin\alpha \leqslant d$, 亦即角度满足 $0 \leqslant \alpha \leqslant \arcsin\frac{d}{\ell}$, 概率就是相同的: $\frac{\ell \sin\alpha}{d}$. 但若角度 α 更大, 针就必定穿过横线, 故概率是 1. 从而对 $\ell \geqslant d$ 计算得

$$\begin{aligned} p &= \frac{2}{\pi}\Big(\int_0^{\arcsin(d/\ell)} \frac{\ell \sin\alpha}{d}\, d\alpha + \int_{\arcsin(d/\ell)}^{\pi/2} 1\, d\alpha\Big) \\ &= \frac{2}{\pi}\Big(\frac{\ell}{d}\big[-\cos\alpha\big]_0^{\arcsin(d/\ell)} + \Big(\frac{\pi}{2} - \arcsin\frac{d}{\ell}\Big)\Big) \\ &= 1 + \frac{2}{\pi}\Big(\frac{\ell}{d}\Big(1 - \sqrt{1 - \frac{d^2}{\ell^2}}\Big) - \arcsin\frac{d}{\ell}\Big). \end{aligned}$$

由此可见, 长针的答案不那么漂亮, 但它提供给我们一些有益的练习: 证明 ("安全起见") 以上公式在 $\ell = d$ 时得出 $\frac{2}{\pi}$, 概率依 ℓ 严格递增, 以及当 $\ell \longrightarrow \infty$ 时概率趋于 1.

参考文献

[1] E. Barbier: *Note sur le problème de l'aiguille et le jeu du joint couvert,* J. Mathématiques Pures et Appliquées (2) **5** (1860), 273-286.

[2] L. Berggren, J. Borwein & P. Borwein, eds.: *Pi: A Source Book,* Springer-Verlag, New York 1997.

[3] G. L. Leclerc, Comte de Buffon: *Essai d'arithmétique morale,* Appendix to "Histoire naturelle générale et particulière," Vol. 4, 1777.

[4] D. A. Klain & G.-C. Rota: *Introduction to Geometric Probability,* "Lezioni Lincee," Cambridge University Press 1997.

[5] T. H. O'Beirne: *Puzzles and Paradoxes,* Oxford University Press, London 1965.



"有麻烦了?"

组合数学



"沉思的拉丁方"

鸽笼与双计数

第 22 章

一些数学原理, 比方说本章标题中的两个, 是如此显然, 以致于人们或许以为其只能给出同样明显的结果. 为说服人们 “那可不一定”, 我们演示一些 Paul Erdős 建议的包含在数学天书中的例子, 而在后几章也会再遇到它们.

鸽笼原理.
若把 n 个物体放在 r 个盒子里, $r < n$, 那么至少有一个盒子包含多于一个物体.

好, 这的确显然, 没什么需要证的. 用映射的语言则可以这样叙述我们的原理: 设 N 和 R 是两个有限集合且

$$|N| = n > r = |R|,$$

再令 $f : N \longrightarrow R$ 为一个映射, 则存在某个 $a \in R$ 使得 $|f^{-1}(a)| \geqslant 2$. 我们还可以讲一个更强的不等式: 存在某个 $a \in R$ 使得

$$|f^{-1}(a)| \geqslant \left\lceil \frac{n}{r} \right\rceil. \quad (1)$$

事实上, 否则的话将对所有的 a 有 $|f^{-1}(a)| < \frac{n}{r}$, 从而 $n = \sum_{a\in R} |f^{-1}(a)| < r\frac{n}{r} = n$, 矛盾.



“一只鸟眼中的鸽笼”

1. 数

断言. 考虑数 $1, 2, 3, \cdots, 2n$, 任取其中的 $n+1$ 个, 则这 $n+1$ 个数中必有两个彼此互素.

这仍是显然的. 一定有两个数彼此只差 1, 从而互素.

现在让我们把问题反过来.

断言. 仍设 $A \subseteq \{1, 2, \cdots, 2n\}$ 且 $|A| = n+1$, 则 A 中总有两个数使得其中一个能被另一个整除.

这就不那么显然了. 根据 Erdős 所说, 他在吃饭的时候把这个问题讲给年轻的 Lajos Pósa, 餐毕 Lajos 就有了答案. 这个问题始终在 Erdős 最欣赏的数学 "启蒙" 问题之列. 是鸽笼原理为它提供了 (肯定的) 答案. 记每个数 $a \in A$ 形如 $a = 2^k m$, 其中 m 是 1 与 $2n-1$ 之间的奇数. 由于 A 里有 $n+1$ 个数, 但仅存在 n 个不同的奇数部分, A 里就至少存在两个数有相同的奇数部分. 从而某个数是另一个的倍数. □

若将 $n+1$ 替换为 n, 两个结果都将不再为真: 为此分别考虑集合 $\{2,4,6,\cdots,2n\}$ 与 $\{n+1,n+2,\cdots,2n\}$.

2. 序列

这是 Erdős 的另一件珍宝, 它来自 Erdős 和 Szekeres 关于 Ramsey 问题的一篇文章.

断言. 在由任意 $mn+1$ 个互异的实数组成的序列 $a_1,a_2,\cdots,a_{mn+1}$ 中, 要么存在一个长为 $n+1$ 的递增子序列

$$a_{i_1} < a_{i_2} < \cdots < a_{i_{m+1}} \qquad (i_1 < i_2 < \cdots < i_{m+1}),$$

要么存在一个长为 $n+1$ 的递减子序列

$$a_{j_1} > a_{j_2} > \cdots > a_{j_{n+1}} \qquad (j_1 < j_2 < \cdots < j_{n+1}),$$

也可能两者都存在.

这一次稍缓再应用鸽笼原理. 对每个 a_i, 令 t_i 表示从 a_i 开始的最长递增子序列的长度. 若存在某个 i, 使得 $t_i \geqslant m+1$, 则我们有了长为 $m+1$ 的递增子序列. 那么假设对所有的 i, 有 $t_i \leqslant m$. 函数 $f: a_i \longmapsto t_i$ 把 $\{a_1,\cdots,a_{mn+1}\}$ 映到 $\{1,\cdots,m\}$ 里面这一事实则告诉我们: 根据 (1), 存在 $s \in \{1,\cdots,m\}$ 使得对某 $\frac{mn}{m}+1 = n+1$ 个数 a_i 有 $f(a_i)=s$. 令 $a_{j_1},a_{j_2},\cdots,a_{j_{n+1}}$ $(j_1 < \cdots < j_{n+1})$ 表示这些数. 观察连续的两个数 $a_{j_i}, a_{j_{i+1}}$. 若 $a_{j_i} < a_{j_{i+1}}$, 取从 $a_{j_{i+1}}$ 开始长为 s 的递增子序列, 则存在从 a_{j_i} 开始的长为 $s+1$ 的递增子序列. 由 $f(a_{j_i}) = s$, 这不可能. 我们于是得到了一个长为 $n+1$ 的递减子序列 $a_{j_1} > a_{j_2} > \cdots > a_{j_{n+1}}$. □

读者或许乐于证明对 mn 个数上面的命题不再成立.

这个关于单调序列的看似简单的结果有一个相当深刻的在图的维数上的推论. 这里无需介绍一般图的维数概念, 而仅仅定义完全图 K_n 的维数, 描述如下: 令 $N = \{1,\cdots,n\}$, $n \geqslant 3$, 考虑 N 上的 m 个置换 $\pi_1,\cdots,\pi_m$. 称这些置换 π_i *表示* K_n, 如果对任意三个互异的数 i,j,k 存在置换 π 使得 k 在 i 与 j *之后*. K_n 的维数就是使得有表示 $\pi_1,\cdots,\pi_m$ 存在的最小的 m.

例如 $\dim(K_3) = 3$, 因为三个数字都必须在最后位置出现一次: $\pi_1 = (1,2,3)$, $\pi_2 = (2,3,1)$, $\pi_3 = (3,1,2)$. 那么 K_4 呢? 首先注意 $\dim(K_n) \leqslant \dim(K_{n+1})$: 仅在 K_{n+1} 的表示里删去 $n+1$. 故 $\dim(K_4) \geqslant 3$, 而事实上通过取

$$\pi_1 = (1,2,3,4), \quad \pi_2 = (2,4,3,1), \quad \pi_3 = (1,4,3,2)$$

可知 $\dim(K_4) = 3$. 不难证明 $\dim(K_5) = 4$, 但是接着令人惊奇的是直到 $n = 12$ 维数一直停留在 4, 然后 $\dim(K_{13}) = 5$.

π_1:	1	2	3	5	6	7	8	9	10	11	12	4
π_2:	2	3	4	8	7	6	5	12	11	10	9	1
π_3:	3	4	1	11	12	9	10	6	5	8	7	2
π_4:	4	1	2	10	9	12	11	7	8	5	6	3

这四个置换表示 K_{12}

所以 $\dim(K_n)$ 看起来是个很难控制的函数. 不过并非如此! 当 n 趋于无穷, $\dim(K_n)$ 事实上是个很好的函数 —— 找到下界的关键是鸽笼原理. 我们断言

$$\dim(K_n) \geqslant \log_2 \log_2 n. \tag{2}$$

由于我们看到 $\dim(K_n)$ 关于 n 单调, 故只需对 $n = 2^{2^p} + 1$ 验证 (2), 即证明

$$\dim(K_n) \geqslant p+1, \qquad \text{当} \quad n = 2^{2^p} + 1.$$

假设不然, $\dim(K_n) \leqslant p$. 令 $\pi_1, \cdots, \pi_p$ 为 $N = \{1, 2, \cdots, 2^{2^p} + 1\}$ 的表示置换. 现在我们连续 p 次应用关于单调子序列的结果. 在 π_1 中必存在长度为 $2^{2^{p-1}} + 1$ 的单调子序列 A_1 (递增或递减并不重要). 在 π_2 中考察集合 A_1 中的元素, 再用一次单调子序列的结果, 找到 π_2 中 A_1 的长为 $2^{2^{p-2}} + 1$ 的单调子序列 A_2, A_2 中的元素当然也在 π_1 中单调. 继续下去, 最终找到一个大小为 $2^{2^0} + 1 = 3$ 的子序列 A_p, 它在所有的 置换 π_i 中都单调. 令 $A_p = (a, b, c)$, 则在所有的 π_i 中或者 $a < b < c$, 或者 $a > b > c$. 但这是不可能的, 因为本该有个置换使得 b 出现在 a 和 c 之后. □

正确的渐进增长率由 Joel Spencer (上界) 和 Füredi, Hajnal, Rödl 与 Trotter (下界) 给出:

$$\dim(K_n) = \log_2 \log_2 n + (\frac{1}{2} + o(1)) \log_2 \log_2 \log_2 n.$$

但这还不是全部. 最近, Morris 和 Hoşten 找到了一种方法, 本质上建立了 $\dim(K_n)$ 的*确切*值. 利用他们的结果和计算机, 我们就得到边栏上的那些值. 这真了不起! 只要想想大小为 1422564 的置换有多少个. 判断 7 个抑或 8 个置换刚好可以表示 $K_{1422564}$ 该是多么困难啊?

$\dim(K_n) \leqslant 4 \iff n \leqslant 12$
$\dim(K_n) \leqslant 5 \iff n \leqslant 81$
$\dim(K_n) \leqslant 6 \iff n \leqslant 2646$
$\dim(K_n) \leqslant 7 \iff n \leqslant 1422564$

3. 求和

Paul Erdős 把下面这个鸽笼原理的漂亮应用归功于 Andrew Vázsonyi 和 Marta Sved:

断言. 给定 n 个不一定互异的整数 $a_1, \cdots, a_n$, 则必存在连续的整数 $a_{k+1}, a_{k+2}, \cdots, a_\ell$, 其和 $\sum_{i=k+1}^{\ell} a_i$ 是 n 的倍数.

置 $N = \{0, 1, \cdots, n\}$ 及 $R = \{0, 1, \cdots, n-1\}$. 考虑映射 $f : N \to R$, 其中 $f(m)$ 是 $a_1 + \cdots + a_m$ 被 n 除的余数. 由 $|N| = n+1 > n = |R|$, 一定存在两个和 $a_1 + \cdots + a_k$, $a_1 + \cdots + a_\ell$ $(k < \ell)$ 有相同的余数. 以上第 1 个和可能是空的, 此时取为 0. 于是

$$\sum_{i=k+1}^{\ell} a_i = \sum_{i=1}^{\ell} a_i - \sum_{i=1}^{k} a_i$$

余数为 0. 证毕. □

让我们转向第二条原理: 使用两种方法计数. 这指的是以下的方法.

双计数.
设给定了两个有限的集合 R 与 C 以及子集 $S \subseteq R \times C$. 当 $(p, q) \in S$ 时, 我们称 p 和 q 是关联的. 令 r_p 表示和 $p \in R$ 关联的元素数, c_q 表示和 $q \in C$ 关联的元素数, 那么

$$\sum_{p \in R} r_p = |S| = \sum_{q \in C} c_q. \tag{3}$$

不证自明: 第一个和把 S 里的对按照第一个元素分类, 第二个和按照第二个元素分类.

把集合 S 画出来是个好办法. 考虑矩阵 S 的关联矩阵 $A = (a_{pq})$, 其行和列分别由 R 与 C 里的元素标记, 使得

$$a_{pq} = \begin{cases} 1 & 当 (p, q) \in S \\ 0 & 当 (p, q) \notin S. \end{cases}$$

如此设置, 可见 r_p 是 A 的第 p 行元素的和, 而 c_q 是第 q 列元素之和. 因此 (3) 的第一个和把 A 的元素按行加起来 (即对 S 的元素计数), 第二个和则是按列加起来.

下面的例子应该可以说明这个对应. 令 $R = C = \{1, 2, \cdots, 8\}$, 且置 $S = \{(i, j) : i|j\}$, 于是得到边栏的矩阵 (只显示非零的元素 1).

R \ C	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2		1		1		1		1
3			1			1		
4				1				1
5					1			
6						1		
7							1	
8								1

4. 仍旧是数

看边栏的表: 第 j 列里 1 的个数恰为 j 的因子数, 用 $t(j)$ 标记之. 现在问当 j 从 1 增加到 $n, t(j)$ 平均有多大? 此即要求量

$$\bar{t}(n) = \frac{1}{n}\sum_{j=1}^{n} t(j).$$

对一般的 $n, \bar{t}(n)$ 是多大? 乍看上去颇为无助. 当 p 是素数, 有 $t(p) = 2$; 而对 2^k 却有很大的值 $t(2^k) = k + 1$. 所以 $t(n)$ 跳动剧烈, 这让我们怀疑 $\bar{t}(n)$ 也差不多如此. 事实正相反! 双计数的方法给出了一个意外而漂亮的答案.

对整数 1 到 n 考虑 (如上的) 矩阵 A, 按列计数得到 $\sum_{j=1}^{n} t(j)$. 那么第 i 行有多少个 1 呢? 非常简单, 这些 1 对应 i 的倍数: $1i, 2i, \cdots$, 而最后一个不超过 n 的倍数是 $\lfloor \frac{n}{i} \rfloor i$. 因此

$$\bar{t}(n) \;=\; \frac{1}{n}\sum_{j=1}^{n} t(j) \;=\; \frac{1}{n}\sum_{i=1}^{n}\left\lfloor\frac{n}{i}\right\rfloor \leqslant \frac{1}{n}\sum_{i=1}^{n}\frac{n}{i} \;=\; \sum_{i=1}^{n}\frac{1}{i}.$$

n	1	2	3	4	5	6	7	8
$\bar{t}(n)$	1	$\frac{3}{2}$	$\frac{5}{3}$	2	2	$\frac{7}{3}$	$\frac{16}{7}$	$\frac{5}{2}$

$\bar{t}(n)$ 的几个初始值

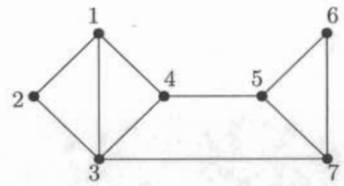
以上当每一项由 $\lfloor \frac{n}{i} \rfloor$ 近似为 $\frac{n}{i}$, 误差不超过 1. 现在最后一个和是第 n 个调和数 H_n, 因此有 $H_n - 1 < \bar{t}(n) < H_n$. 参考第 2 章对 H_n 的估计就有

$$\log n - 1 \;<\; H_n - 1 - \frac{1}{n} \;<\; \bar{t}(n) \;<\; H_n \;<\; \log n + 1.$$

于是我们证明了这个非凡的结论, 尽管 $t(n)$ 飘忽不定, 均值 $\bar{t}(n)$ 却表现优美: 它和 $\log n$ 上下只差不到 1.

5. 图

令 G 为有限简单图, 其顶点集为 V, 边集为 E. 在第 11 章我们已经定义了顶点 v 的度 $d(v)$: 即以 v 为一个端点的边的数目. 图中的例子里, 各顶点 $1, 2, \cdots, 7$ 分别具有度数 $3, 2, 4, 3, 3, 2, 3$.



大部分图论书以下面的结果开头 (事实上我们已在第 11, 17 章见过了):

$$\sum_{v \in V} d(v) \;=\; 2|E|. \tag{4}$$

考察 $S \subseteq V \times E$, 其中 S 是对 (v, e) 的集合, 要求 $v \in V$ 是 $e \in E$ 的一个端点. 对 S 双计数一方面给出 $\sum_{v \in V} d(v)$, 因为每个顶点对和贡献了 $d(v)$ 那么多; 另一方面给出 $2|E|$, 因为每条边有两个端点. □

结果 (4) 看上去如此简单, 却有许多重要的推论, 我们在下文中将讨论其中的一些. 本节则挑出一个对图的极值问题的优美应用, 问题如下:

假设 $G = (V, E)$ 是一个具有 n 个顶点但不含长度为 4 的圈 (记为 C_4) 的图, 亦即不含子图  *. 那么 G 最多可以有多少条边?*



例如, 边栏中 5 个顶点的图不含 4- 圈且有 6 条边. 读者容易验证: 在 5 个顶点的情况下最多可能的边数就是 6, 而且该图事实上是唯一的 5 个顶点、6 条边而又没有 4- 圈的图.

现在看一般的情形. 令 G 为 n 个顶点的不含 4- 圈的图. 如上用 $d(u)$ 表示 u 的度数. 现在对集合 S 用两种方法计数: S 是对 $(u, \{v, w\})$ 的集合, 其中 u 与 v 和 u 与 w 都相邻, 且 $v \neq w$. 换言之, 对所有的



进行计数. 关于 u 求和, 我们得到 $|S| = \sum_{u \in V} \binom{d(u)}{2}$. 另一方面, 每个对 $\{v, w\}$ 有至多一个邻居 (由不含 C_4 的条件). 所以 $|S| \leqslant \binom{n}{2}$, 从而

$$\sum_{u \in V} \binom{d(u)}{2} \leqslant \binom{n}{2}$$

或者说

$$\sum_{u \in V} d(u)^2 \leqslant n(n-1) + \sum_{u \in V} d(u). \tag{5}$$

下面 (在这个类型的极值问题中相当典型) 针对向量 $(d(u_1), \cdots, d(u_n))$ 和 $(1, 1, \cdots, 1)$ 应用 Cauchy-Schwarz 不等式, 得

$$\Big(\sum_{u \in V} d(u)\Big)^2 \leqslant n \sum_{u \in V} d(u)^2,$$

从而由 (5),

$$\Big(\sum_{u \in V} d(u)\Big)^2 \leqslant n^2(n-1) + n \sum_{u \in V} d(u).$$

应用 (4) 我们发现

$$4|E|^2 \leqslant n^2(n-1) + 2n|E|$$

或

$$|E|^2 - \frac{n}{2}|E| - \frac{n^2(n-1)}{4} \leqslant 0.$$

解对应的二次方程我们就得到下面的 Istvan Reiman 的结果.

定理. *若 n 个顶点的图 G 不含 4- 圈作为子图, 则*

$$|E| \ \leqslant \ \left\lfloor \frac{n}{4}\left(1+\sqrt{4n-3}\right) \right\rfloor. \tag{6}$$

当 $n=5$ 有 $|E| \leqslant 6$, 上面给出的图表明等号可以成立.

双计数如此容易地给出了边数的一个上界. 一般地, (6) 这个界有多好呢? 下面的美妙例子 [2] [3] [6] 表明, 它几乎是确界. 在这类问题上, 有限几何经常提供帮助.

介绍这个例子时我们假设读者熟悉整数模素数 p 得到的有限域 $\mathbb{Z}_p$ (参看第 4 章). 考虑 $\mathbb{Z}_p$ 上的三维线性空间 X, 通过 X 构造下面的图 G_p. G_p 的顶点是一维子空间 $[\boldsymbol{v}] := \text{span}_{\mathbb{Z}_p}\{\boldsymbol{v}\}, \mathbf{0} \neq \boldsymbol{v} \in X$, 且两个这样的子空间 $[\boldsymbol{v}], [\boldsymbol{w}]$ 有边相连当

$$\langle \boldsymbol{v}, \boldsymbol{w} \rangle \ = \ v_1w_1 + v_2w_2 + v_3w_3 \ = 0.$$

注意从子空间取哪个 $\neq \mathbf{0}$ 的向量并不关键. 用几何的话说, 顶点就是 $\mathbb{Z}_p$ 上 射影空间的点, 而当 $\boldsymbol{w}$ 落在 $\boldsymbol{v}$ 的极线上时 $[\boldsymbol{w}]$ 与 $[\boldsymbol{v}]$ 相邻.

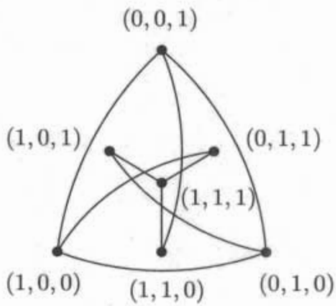


图 G_2: 其顶点是 7 个非零三元组 (x, y, z).

例如图 G_2 不含 4- 圈, 有 9 条边, 几乎达到了 (6) 给出的界 10. 我们将证明这对任意的素数 p 是对的.

先证 G_p 满足不含 C_4 的条件. 若 $[\boldsymbol{u}]$ 是 $[\boldsymbol{v}]$ 和 $[\boldsymbol{w}]$ 的共同邻点, 则 $\boldsymbol{u}$ 是线性方程组

$$\begin{aligned} v_1x + v_2y + v_3z &= 0 \\ w_1x + w_2y + w_3z &= 0 \end{aligned}$$

的解. 由于 $\boldsymbol{v}$ 和 $\boldsymbol{w}$ 线性无关, 解空间维数是 1, 从而公共邻点 $[\boldsymbol{u}]$ 是唯一的.

下面看 G_p 的顶点数, 仍用双计数. 空间 X 包含 p^3-1 个 $\neq \mathbf{0}$ 的向量. 由于每个一维子空间含 $p-1$ 个 $\neq \mathbf{0}$ 的向量, 可知 X 有 $\frac{p^3-1}{p-1} = p^2+p+1$ 个一维子空间, 即 G_p 有 $n = p^2+p+1$ 个顶点. 类似地, 每个二维子空间含 p^2-1 个 $\neq \mathbf{0}$ 的向量, 因此包含 $\frac{p^2-1}{p-1} = p+1$ 个一维子空间.

剩下要决定的是 G_p 的边数, 或者由 (4), 只需知道度数. 由 G_p 的构造, 和 $[\boldsymbol{u}]$ 相邻的顶点都是方程

$$u_1x \ + \ u_2y \ + \ u_3z \ = \ 0 \tag{7}$$

的解. (7) 的解空间是个二维子空间, 所以有 $p+1$ 个顶点与 $[\boldsymbol{u}]$ 相邻. 但须谨慎, $\boldsymbol{u}$ 本身可能也是 (7) 的解, 那将导致仅有 p 个顶点与 $[\boldsymbol{u}]$ 相邻.

总结一下, 我们得到了以下结果: 若 $\boldsymbol{u}$ 落在锥线 $x^2+y^2+z^2=0$ 之上, 则 $d([\boldsymbol{u}])=p$, 否则 $d([\boldsymbol{u}])=p+1$. 因此, 剩下的任务就是找到落在锥线

$$x^2+y^2+z^2=0$$

上的一维子空间的数目. 让我们先看一下这个结果, 稍后再证明.

断言. *方程 $x^2+y^2+z^2=0$ 的解 (x,y,z) 恰有 p^2 个, 所以 (排除零解) G_p 恰有 $\frac{p^2-1}{p-1}=p+1$ 个度数为 p 的顶点.*

利用这个结果就可以结束对 G_p 的分析. 度数为 p 的顶点有 $p+1$ 个, 因此度数为 $p+1$ 的顶点就有 $(p^2+p+1)-(p+1)=p^2$ 个. 利用 (4), 我们得到

$$\begin{aligned} |E| &= \frac{(p+1)p}{2}+\frac{p^2(p+1)}{2}=\frac{(p+1)^2p}{2} \\ &= \frac{(p+1)p}{4}(1+(2p+1)) = \frac{p^2+p}{4}\left(1+\sqrt{4p^2+4p+1}\right). \end{aligned}$$

置 $n=p^2+p+1$, 最后一个方程化为

$$|E|=\frac{n-1}{4}\left(1+\sqrt{4n-3}\right),$$

这几乎与 (6) 吻合.

现在证明断言. 以下的论证是线性代数的优美应用, 用到了对称矩阵和特征值. 在第 34 章我们还会看到这种方法, 这并非巧合: 两个证明出自 Erdős, Rényi 和 Sós 的同一篇文章.

用 $\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_{p^2+p+1}$ 表示前述 X 的一维子空间, 它们两两线性无关. 类似地, 可以用相同的这些向量标记二维子空间, 对应于 $\boldsymbol{u}=(u_1,u_2,u_3)$ 的子空间就是 (7) 中方程 $u_1x+u_2y+u_3z=0$ 的解集. (这当然不过就是线性代数中的对偶原理.) 所以根据 (7), 由 $\boldsymbol{v}_i$ 表示的一维子空间包含在由 $\boldsymbol{v}_j$ 表示的二维子空间里面当且仅当 $\langle \boldsymbol{v}_i,\boldsymbol{v}_j\rangle=0$.

现在考虑如下定义的 $(p^2+p+1)\times(p^2+p+1)$ 矩阵 $A=(a_{ij})$: A 的行与列都对应 $\boldsymbol{v}_1,\cdots,\boldsymbol{v}_{p^2+p+1}$ (对行列也这样标记), 且

$$a_{ij}:=\begin{cases} 1, & 当\ \langle \boldsymbol{v}_i,\boldsymbol{v}_j\rangle=0, \\ 0, & 否则. \end{cases}$$

$$A=\begin{pmatrix} 0&1&1&1&0&0&0\\ 1&0&1&0&1&0&0\\ 1&1&0&0&0&1&0\\ 1&0&0&1&0&0&1\\ 0&1&0&0&1&0&1\\ 0&0&1&0&0&1&1\\ 0&0&0&1&1&1&0 \end{pmatrix}$$

G_2 的矩阵

A 是实对称矩阵, 且当 $\langle v_i, v_i\rangle = 0$, 即当 v_i 在锥线 $x^2+y^2+z^2=0$ 上时, $a_{ii}=1$. 于是只需证明

$$\operatorname{tr}(A) \;=\; p+1.$$

线性代数告诉我们迹 tr (A) 等于特征值之和. 诀窍在这里: 尽管 A 看上去麻烦, 矩阵 A^2 却很容易分析. 注意两个事实:

- A 的每行恰含 $p+1$ 个 1. 这表明 $p+1$ 是 A 的特征值, 因为 $A\mathbf{1} = (p+1)\mathbf{1}$, 这里 $\mathbf{1}$ 是全由 1 组成的向量.
- 对于任两个相异的行 v_i, v_j, 恰有 1 列与这两行相交处都是 1 (这个列对应 v_i, v_j 生成的唯一的那个二维子空间).

由以上事实, 知

$$A^2 = \begin{pmatrix} p+1 & 1 & \cdots & 1 \\ 1 & p+1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & p+1 \end{pmatrix} \;=\; pI + J,$$

其中 I 是单位矩阵, J 是元素全为 1 的矩阵. 现在, J 有特征值 p^2+p+1 (1 重) 和 0 (p^2+p 重). 故 A^2 有 1 重的特征值 $p^2+2p+1=(p+1)^2$ 和 p^2+p 重的特征值 p. 由于 A 是实对称矩阵, 可以对角化, 我们发现 A 有特征值 $p+1$ 或 $-(p+1)$ 及总计 p^2+p 重的特征值 $\pm\sqrt{p}$. 由上面的第一个事实, 最大特征值必定是 $p+1$. 设 $\sqrt{p}$ 是 r 重, 而 $-\sqrt{p}$ 是 s 重的, 则

$$\operatorname{tr}(A) \;=\; (p+1) + r\sqrt{p} - s\sqrt{p}.$$

由于迹是整数, 一定有 $r=s$, 故 tr $(A) = p+1$. 这样我们就达到目的了. □

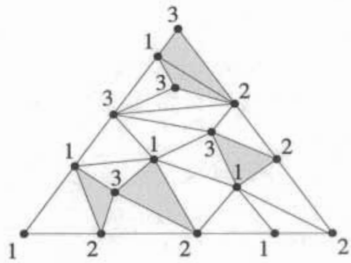
6. Sperner 引理

1912 年, Luitzen Brouwer 发表了著名的不动点定理:

每个从 n 维球到它自身的连续函数 $f\colon B^n \longrightarrow B^n$ 都有不动点 (满足 $f(x)=x$ 的点 $x\in B^n$).

1 维是区间的情形, 从中值定理易得. 但对高维的情形 Brouwer 的证明用到了复杂的工具. 所以发生在 1928 年的如下事情着实令人惊讶: 年轻的 Emanuel Sperner (时年 23 岁) 给出了一个简洁的组合结果, Brouwer 的不动点定理和连续双射的维数不变量都可以从中推得. 此外, 与 Sperner 的精巧引理般配的是它同样美丽的证明——用的是双计数.

以下讨论 Sperner 引理; Brouwer 定理的第一个非平凡情形, 即 $n=2$ 时的情形, 将作为推论. 读者将之推广为更高维数的情形应该不会遇到困难 (对维数归纳).



三着色的三角形用阴影标记

Sperner 引理.

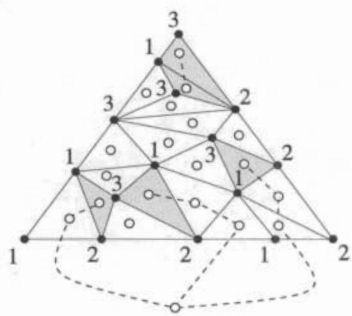
假设顶点为 V_1, V_2, V_3 的 "大" 三角形被三角剖分 (即分解为有限多个拼在一起的 "小" 三角形).

设将三角剖分后的顶点用集合 $\{1,2,3\}$ 中的数 "着色": V_i 得到颜色 i (对每个 i), 沿着 V_i 到 V_j 的边上仅有颜色 i 和 j 被用到 $(i \neq j)$, 但内部的顶点选取颜色 1, 2 或 3 是任意的.

那么一定存在 "三着色" 的小三角形, 其顶点得到了全部的三种颜色.

■ **证明.** 我们证一个更强的结论: 三着色的三角形数不仅不是 0, 而且永远是奇的.

考虑三角剖分图的对偶图, 但不取全部的对偶边, 而只保留那些当它穿过的边的两个端点着色分别是 (不同的)1 和 2 的对偶边. 这样我们得到一个 "部分对偶图": 其顶点的度为 1, 若对应的是三着色的三角形; 度为 2, 若对应的三角形仅有两种颜色 1 和 2; 度为 0, 若对应的三角形里颜色 1 和 2 不都出现. 于是只有三着色的三角形对应奇度数的顶点 (度为 1).



然而, 对偶图里对应三角剖分图外部区域的顶点是奇度的: 事实上沿着长边 V_1 到 V_2, 在颜色 1 与颜色 2 之间变化了奇数次. 所以部分对偶图有奇数条边穿过这条长边, 并且其他两条长边都不同时含有颜色 1 和 2.

现在由于任何有限图里的奇度点是偶数个 (根据方程 (4)), 三着色的小三角形 (对应对偶图内部的那奇数个奇度顶点) 必有奇数个. □

利用这个引理, 容易导出 Brouwer 的定理.

■ **Brouwer 不动点定理的证明.** (当 $n=2$). 令 Δ 为 $\mathbb{R}^3$ 中以 $e_1=(1,0,0)$, $e_2=(0,1,0)$ 和 $e_3=(0,0,1)$ 为顶点的三角形. 因为 Δ 同胚于二维球 B_2, 只需证明每个连续映射 $f: \Delta \longrightarrow \Delta$ 都有不动点.

令 $\delta(\mathcal{T})$ 表示三角剖分 $\mathcal{T}$ 里最长边的长度. 容易构造一个 Δ 的三角剖分的无穷序列 $\mathcal{T}_1, \mathcal{T}_2, \cdots$ 使得最大长度组成的数列 $\delta(\mathcal{T}_k)$ 收敛到 0. 这样的序列可以直接构造, 也可以归纳地构造, 例如令 $\mathcal{T}_{k+1}$ 为 $\mathcal{T}_k$ 按照重心细分.

对每个这样的三角剖分, 给它们的顶点 $\boldsymbol{v}$ 进行 三着色: $\lambda(\boldsymbol{v}) := \min\{i : f(\boldsymbol{v})_i < v_i\}$, 即 $\lambda(\boldsymbol{v})$ 是最小的 i 使得 $f(\boldsymbol{v}) - \boldsymbol{v}$ 的第 i 个坐标是负的. 只要 f 没有不动点, 这个定义就是合理的. 这是因为每个 $\boldsymbol{v} \in \Delta$ 都在平面 $x_1 + x_2 + x_3 = 1$ 上, 所以 $\sum_i v_i = 1$. 因此若 $f(\boldsymbol{v}) \neq \boldsymbol{v}$, 则点 $f(\boldsymbol{v}) - \boldsymbol{v}$ 至少有一个坐标是负的 (也至少有一个坐标是正的).

先验证这个着色满足 Sperner 引理的条件. 首先, 顶点 $\boldsymbol{e}_i$ 必为颜色 i, 因为 $f(\boldsymbol{e}_i) - \boldsymbol{e}_i$ 可能为负的坐标仅有第 i 个. 其次, 若 $\boldsymbol{v}$ 落在与 $\boldsymbol{e}_i$ 相对的长边上, 则 $v_i = 0$, 所以 $f(\boldsymbol{v}) - \boldsymbol{v}$ 的第 i 个坐标不可能是负的, 也就是说 $\boldsymbol{v}$ 不会具有颜色 i.

Sperner 引理于是告诉我们在每个三角剖分 T_k 里面都存在三着色的三角形 $\{\boldsymbol{v}^{k:1}, \boldsymbol{v}^{k:2}, \boldsymbol{v}^{k:3}\}$ 使得 $\lambda(\boldsymbol{v}^{k:i}) = i$. 顶点 $(\boldsymbol{v}^{k:1})_{k\geqslant 1}$ 构成的序列不一定收敛, 但由于单纯形 Δ 是紧的必存在收敛的子序列. 用对应的子序列代替三角剖分 T_k (为方便仍用 T_k 表示), 可设 $(\boldsymbol{v}^{k:1})_k$ 收敛到点 $\boldsymbol{v} \in \Delta$. 另一方面 $\boldsymbol{v}^{k:2}$ 和 $\boldsymbol{v}^{k:3}$ 到 $\boldsymbol{v}^{k:1}$ 的距离最多是 $\delta(T_k)$, 也收敛到 0. 所以点列 $(\boldsymbol{v}^{k:2})$ 和 $(\boldsymbol{v}^{k:3})$ 收敛到相同的点 $\boldsymbol{v}$.

那么 $f(\boldsymbol{v})$ 在哪呢? 已知对所有的 k, $f(\boldsymbol{v}^{k:1})$ 的第一个坐标小于 $\boldsymbol{v}^{k:1}$ 的第一个坐标. 由于 f 连续, $f(\boldsymbol{v})$ 的第一个坐标就小于或等于 $\boldsymbol{v}$ 的第一个坐标. 对第二、第三个坐标也如此. 于是 $f(\boldsymbol{v}) - \boldsymbol{v}$ 的坐标都不是正的, 这与假设 $f(\boldsymbol{v}) \neq \boldsymbol{v}$ 矛盾. □

参考文献

[1] L. E. J. Brouwer: *Über Abbildungen von Mannigfaltigkeiten,* Math. Annalen **71** (1912), 97-115.

[2] W. G. Brown: *On graphs that do not contain a Thomsen graph,* Canadian Math. Bull. **9** (1966), 281-285.

[3] P. Erdős, A. Rényi & V. Sós: *On a problem of graph theory,* Studia Sci. Math. Hungar. **1** (1966), 215-235.

[4] P. Erdős & G. Szekeres: *A combinatorial problem in geometry,* Compositio Math. (1935), 463-470.

[5] S. Hoşten & W. D. Morris: *The order dimension of the complete graph,* Discrete Math. **201** (1999), 133-139.

[6] I. Reiman: *Über ein Problem von K. Zarankiewicz,* Acta Math. Acad. Sci. Hungar. **9** (1958), 269-273.

[7] J. Spencer: *Minimal scrambling sets of simple orders,* Acta Math.

Acad. Sci. Hungar. **22** (1971), 349-353.

[8] E. Sperner: *Neuer Beweis für die Invarianz der Dimensionszahl und des Gebietes,* Abh. Math. Sem. Hamburg **6** (1928), 265-272.

[9] W. T. Trotter: *Combinatorics and Partially Ordered Sets: Dimension Theory,* John Hopkins University Press, Baltimore and London 1992.

有限集上的三个著名定理

第 23 章



Emanuel Sperner

在本章中我们考虑组合数学的一个基本主题: 有限集 $N=\{1,2,\cdots,n\}$ 的一些子集组成的特定集族 $\mathcal{F}$ 的性质和基数. 我们从两个经典结果开始: Sperner 定理和 Erdős-Ko-Rado 定理. 这两个结果的共同特点是它们都被证明了很多遍, 还有它们各自开辟了组合集合论的一个新领域. 看上去归纳法是证明这两个定理的自然途径, 但我们此处要讨论的论证颇为不同而发人深思.

1928 年, Emanuel Sperner 提出并自己解决了这样一个问题: 给定集合 $N=\{1,2,\cdots,n\}$, 称 N 的一些子集构成的集族 $\mathcal{F}$ 为反链, 若 $\mathcal{F}$ 中没有哪个元素是 $\mathcal{F}$ 另一个子集. 反链最大可以是多少? 很明显, 所有的 k- 子集构成的族 $\mathcal{F}_k$ 满足反链的要求, 且 $|\mathcal{F}_k|=\binom{n}{k}$. 在二项式系数中找最大的 (见第 2 章) 可以得到大小为 $\binom{n}{\lfloor n/2\rfloor}=\max_k\binom{n}{k}$ 的反链. Sperner 定理则断言没有更大的了.

定理 1. *一个 n- 集合的最大反链的基数是 $\binom{n}{\lfloor n/2\rfloor}$.*

■ **证明.** 诸多证明中, David Lubell 的那个大概是最简短最优美的了. 设 $\mathcal{F}$ 是任意的一个反链, 往证 $|\mathcal{F}|\leqslant\binom{n}{\lfloor n/2\rfloor}$. 证明的关键是考虑子集组成的链 $\varnothing=C_0\subset C_1\subset C_2\subset\cdots\subset C_n=N$, 且要求当 $i=0,\cdots,n$ 时, $|C_i|=i$ 有多少个链呢? 显然, 可以通过把 N 中的元素一个一个加上去来得到链, 所以刚好有 N 的所有置换那么多个链, 也就是 $n!$. 进一步, 对 $A\in\mathcal{F}$ 研究有多少个链包含 A. 这也容易. 从 $\varnothing$ 到 A 可以把 A 中的元素一个一个加上去, 然后从 A 开始把剩下的元素一个一个加上去直到 N. 故若 A 含 k 个元素, 则合起来就有 $k!(n-k)!$ 个这样的链. 注意不可能有链同时穿过 $\mathcal{F}$ 中两个不同的元素 A 和 B, 因为 $\mathcal{F}$ 是个反链.

为了完成定理的证明, 令 m_k 表示 $\mathcal{F}$ 中的 k- 子集, 则 $|\mathcal{F}|=\sum_{k=0}^{n}m_k$. 根据我们的讨论, 穿过 $\mathcal{F}$ 中某个元素的链的个数为

$$\sum_{k=0}^{n}m_k\,k!\,(n-k)!,$$

而这个数不会超过所有链的数目 $n!$. 所以

$$\sum_{k=0}^{n} m_k \frac{k!(n-k)!}{n!} \leqslant 1 \quad 或 \quad \sum_{k=0}^{n} \frac{m_k}{\binom{n}{k}} \leqslant 1.$$

将分母换为最大的二项式系数, 于是得到

$$\frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \sum_{k=0}^{n} m_k \leqslant 1, \quad 亦即 \quad |\mathcal{F}| = \sum_{k=0}^{n} m_k \leqslant \binom{n}{\lfloor n/2 \rfloor},$$

证毕. □

检验: 当 n 为偶数时所有的 $\frac{n}{2}$- 子集构成的集族, 以及当 n 为奇数时所有的 $\frac{n-1}{2}$- 子集构成的集族和所有的 $\frac{n+1}{2}$- 子集构成的集族确实是仅有的 达到最大基数的反链!

我们的第二个结果则属于完全不同的性质. 仍考虑集合 $N = \{1, \cdots, n\}$. 称子集族 $\mathcal{F}$ 为*相交族*, 若 $\mathcal{F}$ 中任两个元素至少有一个公共元. 几乎可以马上发现最大的相交族的基数为 2^{n-1}: 若$A \in \mathcal{F}$, 那么其补集 $A^c = N \backslash A$ 与 A 相交为空, 故不能出现在 $\mathcal{F}$ 里. 所以相交族最多可以有所有的子集数2^n 的一半那么多的元素, 即 $|\mathcal{F}| \leqslant 2^{n-1}$. 另一方面, 考虑含有某个固定点的所有子集, 例如含有 1 的所有子集构成的族 $\mathcal{F}_1$, 则显然 $|\mathcal{F}_1| = 2^{n-1}$, 问题就解决了.

现在问这么一个问题: 若要求每个子集有同样的基, 比方说 k, 那么 $\mathcal{F}$ 最大可能的基数是多少? 称这样的族为*相交 k- 集族*. 不妨设 $n \geqslant 2k$, 否则任两个 k- 子集必相交, 故无需证明. 用上面的思想, 取含固定点 (如 1) 的所有 k- 子集当然可以得到满足条件的集族 $\mathcal{F}_1$. 显然 $\mathcal{F}_1$ 里的子集可以通过把 1 加到 $\{2, 3, \cdots, n\}$ 所有的 $(k-1)$- 子集里得到, 因此 $|\mathcal{F}_1| = \binom{n-1}{k-1}$. 还可以更优吗? 不 —— 这就是 Erdős-Ko-Rado 定理.

定理 2. *当 $n \geqslant 2k$, 一个 n- 集合的相交 k- 集族最大可能的基数是 $\binom{n-1}{k-1}$.*

1938 年, Paul Erdős, 柯召 (Chao Ko) 和 Richard Rado 发现了这个定理, 但直到 23 年后才将之发表. 此后众多证明和变形纷至沓来, 但下面的由 Gyula Katona 给出的证明格外优雅.

■ **证明.** 证明的关键是一个乍看上去和我们的问题毫不相干的简单引理. 考虑被 n 个点分成 n 条边的圆周 C. 每条长为 k 的弧 包含 $k+1$ 个连续的点和它们之间的 k 条边.



当 $n = 6$ 时的圆周 C. 黑色的几条边描绘出一条长为 3 的圆弧.

引理. *设 $n \geqslant 2k$, 且设有 t 条长为 k 的互异的弧 $A_1, \cdots, A_t$, 使得任两条弧之交非空, 则 $t \leqslant k$.*

为证引理, 注意 C 的每一点至多是某 1 条弧的端点. 事实上, 若 A_i, A_j 有公共的端点 v, 则它们不得不向相反的方向延展 (因为

它们是相异的). 但由 $n \geqslant 2k$ 它们将不会有公共边. 固定 A_1, 由于每个 A_i $(i \geqslant 2)$ 与 A_1 有公共边, A_i 的一个端点是 A_1 的内点. 从上面看出这些端点各不相同, 而 A_1 共有 $k-1$ 个内点, 所以 A_1 之外只能有至多 $k-1$ 条弧, 加起来至多有 k 条弧. 引理得证. □

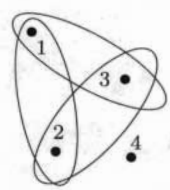
现在继续证明 Erdős-Ko-Rado 定理. 令 $\mathcal{F}$ 是一个相交 k- 集族. 考虑上述有 n 个点, n 条边的圆周 C. 取环排列 $\pi = (a_1, a_2, \cdots, a_n)$, 将 a_i 依顺时针写在 C 的各边上. 对满足其 k 个元素连续地出现在 C 上的集合 $A \in \mathcal{F}$ 计数. 由于 $\mathcal{F}$ 是相交族, 引理告诉我们至多有 k 个这样的集合. 这对所有的环排列都如此, 又因为一共有 $(n-1)!$ 个环排列, 故以上的方式产生了至多

$$k(n-1)!$$

个 $\mathcal{F}$ 中的集合, 其元素连续地出现在某个环排列上. 对固定的集合 $A \in \mathcal{F}$, 我们计数了多少次呢? 很容易: 如果 A 的 k 个元素是按照某种顺序连续出现的, 则 A 出现在 π 里. 而我们共有 $k!$ 种可能连续地书写 A, 以及 $(n-k)!$ 种方式将剩余的元素排序. 因此结论是固定的集合 A 恰好出现在 $k!(n-k)!$ 个环排列里面, 从而

$$|\mathcal{F}| \leqslant \frac{k(n-1)!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} = \binom{n-1}{k-1}. \quad \square$$

我们仍可以问包含某个固定元素的 k- 集族是不是唯一达到最大基数的情形. 当 $n = 2k$ 时这当然不对. 例如, 当 $n = 4$ 及 $k = 2$ 时集族 $\{1,2\}, \{1,3\}, \{2,3\}$ 的基数也是 $\binom{3}{1} = 3$. 一般地, 当 $n = 2k$ 时, 可以通过任意选取 k- 子集 A 与其补集 $N \backslash A$ 这一对中的某一个来得到基数为 $\frac{1}{2}\binom{n}{k} = \binom{n-1}{k-1}$ 的最大相交 k- 集族. 但当 $n > 2k$ 时, 包含某个固定元素的特殊集族确实是唯一的情形了. 读者请试着自己证明.



当 $n = 4, k = 2$ 时的一个相交集族

最后, 我们转向第三个结果, 这或许是有限集合论中最重要的基本定理了: Philip Hall 在 1935 年证明的 "婚姻定理". 它打开了今天所谓匹配理论的大门, 且有广泛的应用, 其中的一些我们随后还会看到.

考察有限集 X 与 X 的子集 $A_1, \cdots, A_n$ (不一定互异). 称序列 $x_1, \cdots, x_n$ 为 $\{A_1, \cdots, A_n\}$ 的一个**相异代表系**, 若 x_i 两两互异, 且对所有的 i 有 $x_i \in A_i$. 简称为 SDR 的这样的一个系统当然未必存在, 例如当某个集合 A_i 是空的. Hall 定理的内容就是关于 SDR 存在的确切条件.



“集体婚礼”

给出结果之前让我们从人的角度阐释一下, 从中明白其俗称 婚姻定理 的缘由: 考虑女孩的集合 $\{1,\cdots,n\}$ 与男孩的集合 X. 当 $x\in A_i$, 女孩 i 与男孩 x 有结婚的可能, 即 A_i 是女孩 i 的所有可能对象的集合. 存在 SDR 则表示存在每一个女孩都得以与自己喜欢的男孩结婚的集体婚配模式.

回到集合, 我们的结果陈述如下:

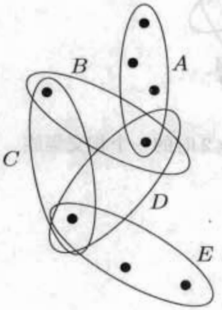
定理 3. 令 $A_1,\cdots,A_n$ 为有限集 X 的一些子集. 它们存在相异代表系当且仅当对每个 $1\leqslant m\leqslant n$, 任意 m 个子集 A_i 的并包含至少 m 个元素.

必要条件是显然的: 若某 m 个集合 A_i 的并含有少于 m 个元素, 则这 m 个集合就不能被互异的元素代表. 令人惊讶的事实 (导致了普适的应用) 是这个明显的条件也是充分的. Hall 的原始证明相当复杂, 随后出现了众多不同的证明, 其中下面这个 (属于 Easterfield, 被 Halmos 和 Vaughan 重新发现的) 也许是最自然的.

■ **证明.** 对 n 归纳. 当 $n=1$ 时显然. 令 $n>1$, 且设 $\{A_1,\cdots,A_n\}$ 满足定理的条件, 该条件以下略为 (H). 对 $1\leqslant \ell<n$, 称 ℓ 个集合 A_i 为临界族, 若它们的并集的基数刚好为 ℓ. 下面我们分两种情形讨论.

情形 1. 不存在临界族.

任取 $x\in A_n$. 从 X 中去掉 x, 考虑集合 $A'_1,\cdots,A'_{n-1}$, 这里 $A'_i=A_i\backslash\{x\}$. 由于不存在临界族, 任意 m 个集合 A'_i 的并仍包含至少 m 个元素. 因此由归纳法知存在 $\{A'_1,\cdots,A'_{n-1}\}$ 的 SDR $x_1,\cdots,x_{n-1}$. 令 $x_n=x$, 合在一起就给出了原来集族的 SDR.



$\{B,C,D\}$ 是一个临界族

情形 2. 存在临界族.

重新排序后可假定 $\{A_1,\cdots,A_\ell\}$ 是临界族, 则有 $\bigcup_{i=1}^{\ell}A_i=\widetilde{X}$ 满足 $|\widetilde{X}|=\ell$. 由 $\ell<n$, 应用归纳可得存在 $A_1,\cdots,A_\ell$ 的 SDR. 即存在 $\widetilde{X}$ 中元素的排序 $x_1,\cdots,x_\ell$ 使得对所有的 $i\leqslant\ell$, 有 $x_i\in A_i$.

考虑剩下的集合 $A_{\ell+1},\cdots,A_n$, 任取它们中的 m 个. 根据条件 (H), $A_1,\cdots,A_\ell$ 和这 m 个集合的并包含至少 $\ell+m$ 个元素, 所以这 m 个集合在 $\widetilde{X}$ 之外还包含至少 m 个元素. 换言之, 集族

$$A_{\ell+1}\backslash\widetilde{X},\ \cdots\ ,A_n\backslash\widetilde{X}$$

也满足条件 (H). 归纳假设给出 $A_{\ell+1},\cdots,A_n$ 的在 $\widetilde{X}$ 之外的一个 SDR.

将其与 $x_1, \cdots, x_\ell$ 合在一起, 我们得到所有集合 A_i 的一个 SDR. 证毕. □

正如我们提到过的, Hall 的定理是如今已很宏大的匹配理论领域的开端 [6]. 在诸多变形和分枝中让我们提一个特别有意思的结果. 我们请读者来自行证明:

> 设集合 $A_1, \cdots, A_n$ 的基数都是 $k \geqslant 1$, 并且没有元素含在多于 k 个集合里, 则存在 k 个 SDR 使得对任意的 i, A_i 的 k 个代表元是互异的, 从而合在一起构成 A_i.

这个美丽的结论或许可以开启新的婚姻模式.

参考文献

[1] T. E. Easterfield: *A combinatorial algorithm,* J. London Math. Soc. **21** (1946), 219-226.

[2] P. Erdős, C. Ko & R. Rado: *Intersection theorems for systems of finite sets,* Quart. J. Math. (Oxford), Ser. (2) **12** (1961), 313-320.

[3] P. Hall: *On representatives of subsets,* J. London Math. Soc. **10** (1935), 26-30.

[4] P. R. Halmos & H. E. Vaughan: *The marriage problem,* Amer. J. Math. **72** (1950), 214-215.

[5] G. Katona: *A simple proof of the Erdős-Ko-Rado theorem,* J. Combinatorial Theory, Ser. B **13** (1972), 183-184.

[6] L. Lovász & M. D. Plummer: *Matching Theory,* Akadémiai Kiadó, Budapest 1986.

[7] D. Lubell: *A short proof of Sperner's theorem,* J. Combinatorial Theory **1** (1966), 299.

[8] E. Sperner: *Ein Satz über Untermengen einer endlichen Menge,* Math. Zeitschrift **27** (1928), 544-548.

洗牌

第 24 章

> 一副牌要洗多少次才会变得随机?

对随机过程的分析是生活中熟识的活动 ("高峰时间开车到机场要多久?"), 数学中也如此. 当然, 得到有意义的答案严重依赖于问题的提法. 就洗牌的问题而言, 这意味着我们必须

- 确定一副牌的数目 (例如 $n = 52$ 张牌),
- 说明洗牌的方式 (我们将先分析顶牌随机插入的洗牌方法, 再分析更实际有效的流插 (riffle) 洗牌), 以及最后
- 解释在怎样的意义下 "随机" 或 "接近随机."

因此本章的目的是分析流插洗牌方法, 这归功于 Edgar N. Gilbert 和 Claude Shannon (1955, 未发表) 以及 Jim Reeds (1981, 未发表). 我们是根据统计学家 David Aldous 和由魔术师改行成为数学家的 Persi Diaconis 的著作 [1]. 我们不会涉及最精确的结果, 即: 7 次流插的确足够将 $n = 52$ 张卡片变得相当接近随机, 而 6 次流插则不行, 但我们将得到上界 12, 而且顺道看见一些极为优美的思想: 停止规则与 "强一致时间" 的概念、强一致时间约束变差距的引理、Reeds 的逆向引理以及由此把洗牌看作 "逆分类" 的阐释. 最后, 所有这些都会归结到两个非常经典的组合问题, 即赠卡收集者和生日悖论. 那么就让我们从这两个问题开始吧!



Persi Diaconis 当魔术师时的名片. 在后来的一次采访中他讲到: "若你自称是斯坦福的教授, 则会受到人们尊重; 但若你说自己是设计魔术戏法的, 他们则想避免你和他们的女儿相识."

生日悖论

随机地取 n 个人, 比方说某门课程或者讨论班的听众. 他们的生日各异的概率是多少? 采用通常的简化假设 (每年 365 天, 不存在季节差异, 没有双胞胎) 这个概率是

$$p(n) = \prod_{i=1}^{n-1}\left(1 - \frac{i}{365}\right).$$

当 $n=23$, 这比 $\frac{1}{2}$ 还小 (所以叫 "生日悖论"!), 当 $n=42$ 时小于百分之 9, 而当 $n>365$ 时就确实为 0 了 ("鸽笼原理", 见第 22 章). 这个公式容易理解 —— 把人们按某个固定的顺序排起来: 若前 i 个人有互异的生日, 那么第 $(i+1)$ 个人不把事情搞砸的概率是 $1-\frac{i}{365}$, 因为还剩下 $365-i$ 个日子可供选择了.

类似地, 若将 n 个球各自独立随机地放到 K 个盒子里, 则没有盒子装了多于 1 个球的概率是

$$p(n,K) \;=\; \prod_{i=1}^{n-1}\Big(1-\frac{i}{K}\Big).$$

赠卡收集者

孩子们买摇滚明星 (或者足球明星) 的照片, 放到自己的影集里. 但是他们买的东西装在不透明的小信封里, 所以不清楚将会得到哪张照片. 如果一共有 n 张不同的照片, 到每张照片收集全一共买下的卡片数的期望是多少呢?

等价地, 从一个装着 n 个不同球的碗中随机选取, 每次取一个球再放回去搅成原状. 平均来讲, 到每个球都被选取至少一次时一共取了多少次球呢?

若已经取过 k 个不同的球, 那么下一次取的不是新球的概率是 $\frac{k}{n}$. 所以需要恰好 s 次选取才得到下一个新球的概率是 $(\frac{k}{n})^{s-1}(1-\frac{k}{n})$. 于是得到下一个新球的期望值是

$$\sum_{s\geqslant 1}\Big(\frac{k}{n}\Big)^{s-1}\Big(1-\frac{k}{n}\Big)s \;=\; \frac{1}{1-\frac{k}{n}},$$

$$\sum_{s\geqslant 1} x^{s-1}(1-x)s \;=$$
$$=\; \sum_{s\geqslant 1} x^{s-1}s \;-\; \sum_{s\geqslant 1} x^{s}s$$
$$=\; \sum_{s\geqslant 0} x^{s}(s+1) \;-\; \sum_{s\geqslant 0} x^{s}s$$
$$=\; \sum_{s\geqslant 0} x^{s} \;=\; \frac{1}{1-x},$$

最终加的是一个几何级数 (见第 6 章).

这个计算可以从边栏的级数里得到. 因此, 把 n 个不同球中的每个都取到至少一次的期望值是

$$\sum_{k=0}^{n-1}\frac{1}{1-\frac{k}{n}} \;=\; \frac{n}{n}+\frac{n}{n-1}+\cdots+\frac{n}{2}+\frac{n}{1} \;=\; nH_n \;\approx\; n\log n.$$

上面的界就是我们在第 2 章得到的调和级数. 所以赠卡收集者问题的答案就是: 我们期待大概需要 $n\log n$ 次选取.

以下的估计是关于需要比 $n\log n$ 显著多次试验的概率. 若 V_n 表示需要的选取次数 (这个随机变量的期望值是 $E[V_n]\approx n\log n$), 则对 $n\geqslant 1$ 和 $c\geqslant 0$, 需要多于 $m:=\lceil n\log n+cn\rceil$ 次选取的概率是

$$\mathrm{Prob}\big[V_n>m\big] \;\leqslant\; e^{-c}.$$

事实上, 若 A_i 表示球 i 没有在前 m 次被选中这一事件, 则

$$\begin{aligned}\text{Prob}[V_n > m] &= \text{Prob}\Big[\bigcup_i A_i\Big] \leqslant \sum_i \text{Prob}[A_i] \\ &= n\Big(1-\frac{1}{n}\Big)^m < ne^{-m/n} \leqslant e^{-c}.\end{aligned}$$

简单的计算表明 $(1-\frac{1}{n})^n$ 关于 n 递增, 且收敛到 $1/e$. 故对任意的 $n \geqslant 1$, 有 $(1-\frac{1}{n})^n < \frac{1}{e}$ 成立.

现在取一副有 n 张卡片的牌. 按它们出现的次序标记 1 到 n, 则标号 "1" 的卡片在最顶上, 而 "n" 在最底下. 令 $\mathfrak{S}_n$ 表示 $1,\cdots,n$ 上的所有置换. 洗牌意味着把某个随机的置换应用到卡片的顺序上去. 理想地, 这应当说是我们把 $\pi \in \mathfrak{S}_n$ 中任意的置换应用到初始顺序 $(1,2,\cdots,n)$ 上, 每一个都有相同的概率 $\frac{1}{n!}$. 那么仅操作一次整副牌就按顺序 $\pi = (\pi(1),\pi(2),\cdots,\pi(n))$ 排列, 而这将是一个完美的随机顺序. 但是实际中发生的并非如此. 实际上, 在洗牌过程中只有某些置换会出现, 也许它们还并不是都有相同的概率, 而这个操作会重复一定的次数. 在那之后, 我们预期或者说希望整副牌至少是 "接近随机" 了.



顶牌随机插入

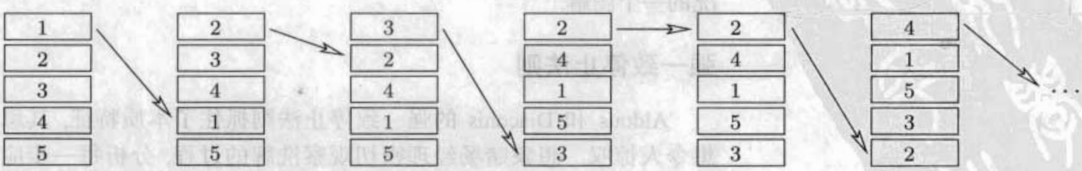
顶牌随机插入洗牌法

如下操作: 取整副牌顶上的那张, 将之插入 n 个不同的可能位置, 每个位置的概率是 $\frac{1}{n}$. 那么就应用了下面置换中的某一个

$$\tau_i = (2,3,\cdots,\underset{\downarrow}{\overset{i}{i}},1,i{+}1,\cdots,n),$$

其中$1 \leqslant i \leqslant n$. 这样洗一次, 看起来整副牌并不随机, 事实上我们期待需要很多次这样的操作才会达到目的.

一种典型的顶牌随机插入的洗牌方式是这样的 (取 $n=5$):



怎样衡量 "接近随机" 呢? 概率学家发明了 "变差距" 作为一种随机程度的度量: 考察整副牌的 $n!$ 个不同排序方式的概率分布, 或者等价地, 对应的 $n!$ 个不同置换 $\sigma \in \mathfrak{S}_n$ 的概率分布.

两个例子是由

$$\begin{aligned} \mathsf{E}(\mathrm{id}) &= 1, \\ \mathsf{E}(\pi) &= 0, \quad \text{其他情况} \end{aligned}$$

给出的初始分布 E, 以及由

$$\mathsf{U}(\pi) = \tfrac{1}{n!}, \quad \text{对所有的 } \pi \in \mathfrak{S}_n$$

给出的均匀分布 U. 两个概率分布 Q_1 与 Q_2 的*变差距*定义如下:

$$\|\mathsf{Q}_1 - \mathsf{Q}_2\| := \tfrac{1}{2} \sum_{\pi \in \mathfrak{S}_n} |\mathsf{Q}_1(\pi) - \mathsf{Q}_2(\pi)|.$$

置 $S := \{\pi \in \mathfrak{S}_n : \mathsf{Q}_1(\pi) > \mathsf{Q}_2(\pi)\}$, 利用 $\sum_\pi \mathsf{Q}_1(\pi) = \sum_\pi \mathsf{Q}_2(\pi) = 1$, 可将上式改写为

$$\|\mathsf{Q}_1 - \mathsf{Q}_2\| = \max_{S \subseteq \mathfrak{S}_n} |\mathsf{Q}_1(S) - \mathsf{Q}_2(S)|,$$

其中 $\mathsf{Q}_i(S) := \sum_{\pi \in S} \mathsf{Q}_i(\pi)$. 显然我们有 $0 \leqslant \|\mathsf{Q}_1 - \mathsf{Q}_2\| \leqslant 1$. 以下, "接近随机" 将被解释为 "到均匀分布有小的变差距". 这里初始分布和均匀分布的变差距相当接近于 1:

$$\|\mathsf{E} - \mathsf{U}\| = 1 - \tfrac{1}{n!}.$$

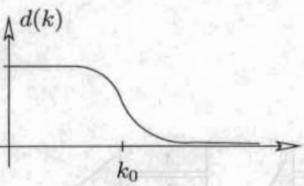
顶牌随机插入一次后, 也没有显著改善:

$$\|\mathsf{Top} - \mathsf{U}\| = 1 - \tfrac{1}{(n-1)!}.$$

对玩牌者来说, 关心的问题不是 "一百万次洗牌后到底离均匀分布多近?", 而是 "洗 7 次牌够了吗?"

(Aldous & Diaconis [1])

在顶牌随机插入 k 次后, $\mathfrak{S}_n$ 上的概率分布记为 Top^{*k}. 那么当 k 变大, 即当我们重复洗牌, $\|\mathsf{Top}^{*k} - \mathsf{U}\|$ 怎样变化呢? 类似地, 其他类型的洗牌方式又如何? 一般理论 (特别地, 有限群上的 Markov 链; 参见 Behrends [3]) 表明对比较大的 k, 变差距 $d(k) := \|\mathsf{Top}^{*k} - \mathsf{U}\|$ 以指数速度收敛到 0, 但不能解释实践中观察到的 "突变" 现象: 进行一定数目 k_0 的洗牌之后, $d(k)$ "突然" 快速收敛到 0. 边白是这种情况的一个图解.



强一致停止法则

Aldous 和 Diaconis 的强一致停止法则抓住了本质特征, 其思想令人惊叹. 想象赌场经理密切观察洗牌的过程, 分析每一步应用到牌上的特定置换, 然后在一些步骤之后根据他观察到的置换喊 "停!". 则他用一个*停止法则*结束了洗牌过程. 这只是依靠已经应用过的 (随机) 置换. 如果对任意的 $k \geqslant 0$ 下面的条件成立, 就称停止规则为*强一致的*:

只要 过程在刚好 k 步后停止, **就有** 得到的置换分布是均匀分布 (确切的!).

令 T 为停止规则告诉经理喊 "停!" 时经历的步数, 则这是个随机变量. 类似地, k 次洗牌后卡片的排序由随机变量 X_k 给出 (在 $\mathfrak{S}_n$ 中取值). 这样, 停止规则是强一致的, 若对所有合适的值 k, 有

$$\text{Prob}\big[X_k = \pi \mid T = k\big] \;=\; \frac{1}{n!} \quad \text{对所有}\pi \in \mathfrak{S}_n.$$

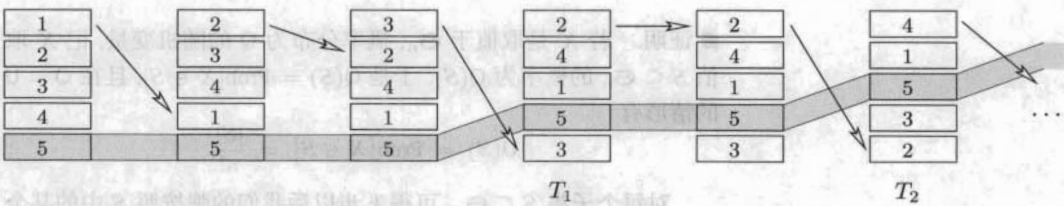
以下三个方面让这个模型有趣, 有用, 且值得注意:

1. 强一致停止规则存在: 很多情形下它们也很简单.
2. 此外, 可以进行分析: 试图决定 $\text{Prob}[T > k]$ 经常引出简单的组合问题.
3. 它会给出变差距, 例如 $d(k) = \|\text{Top}^{*k} - \text{U}\|$ 的有效的上界.

比方说, 顶牌随机插入洗牌法有一个强一致的停止规则

"当最低一张卡片 (标号为 n) 第一次被插回全副牌时, 停止."

事实上, 如果我们在洗牌过程中追踪卡片 n,



则看到整个过程中这张卡片下面的那些牌的顺序是完全一致的. 所以, 当卡片 n 升到最顶端然后再随机地插回来, 整副牌就均匀分布了; 我们只是不知道这件事发生的确切时间 (但是经理看得见).

现在让 T_i 表示第一次有 i 张卡片在 n 下面时所需的洗牌次数这个随机变量. 故须决定

$$T \;=\; T_1 + (T_2 - T_1) + \cdots + (T_{n-1} - T_{n-2}) + (T - T_{n-1})$$

的分布. 但是每一个加项恰好对应着赠卡收集者问题: $T_i - T_{i-1}$ 是顶牌插入到 n 下面的 i 个可能位置的时间. 所以这也是赠卡收集者从第 $(n-i)$ 张照片到第 $(n-i+1)$ 张照片所需的时间. 令 V_i 表示这个人收集到 i 张不同照片时一共买过的赠卡, 则

$$V_n \;=\; V_1 + (V_2 - V_1) + \cdots + (V_{n-1} - V_{n-2}) + (V_n - V_{n-1}).$$

条件概率

条件概率

$$\text{Prob}[A \mid B]$$

表示在事件 B 发生的前提下事件 A 发生的概率. 这恰好是两个事件都发生的概率除以事件 B 为真的概率, 即

$$\text{Prob}[A \mid B] \;=\; \frac{\text{Prob}[A \wedge B]}{\text{Prob}[B]}.$$

且我们已经看到对任意的 i 和 j, 有 $\text{Prob}[T_i - T_{i-1} = j] = \text{Prob}[V_{n-i+1} - V_{n-i} = j]$. 所以赠卡收集者和顶牌随机插入的洗牌者执行的这两个彼此独立的随机过程的序列是等价的, 只不过是相反的方向 (赠卡收集者越往后越难). 因此, 我们知道顶牌随机插入洗牌法的强一致停止规则所需的时间大于 $k = \lceil n \log n + cn \rceil$ 步是以小概率发生的:

$$\text{Prob}\big[T > k\big] \;\leqslant\; e^{-c}.$$

这反过来意味着在 $k = \lceil n \log n + cn \rceil$ 次顶牌随机插入的洗牌后, 我们的牌就 "接近随机" 了, 因为下面的简洁但重要的引理告诉我们

$$d(k) \;=\; \|\mathsf{Top}^{*k} - \mathsf{U}\| \;\leqslant\; e^{-c}.$$

引理. *令 $\mathsf{Q} : \mathfrak{S}_n \longrightarrow \mathbb{R}$ 为任意的概率分布, 其定义了洗牌过程 Q^{*k}; 且有强一致的停止规则, 其停止时间为 T. 则对任意的 $k \geqslant 0$,*

$$\|\mathsf{Q}^{*k} - \mathsf{U}\| \;\leqslant\; \text{Prob}\big[T > k\big].$$

■ **证明.** 若 X 是取值于 $\mathfrak{S}_n$, 概率分布为 Q 的随机变量, 记 X 取值 $S \subseteq \mathfrak{S}_n$ 的概率为 $\mathsf{Q}(S)$. 于是 $\mathsf{Q}(S) = \text{Prob}[X \in S]$, 且在 $\mathsf{Q} = \mathsf{U}$ 的情形有

$$\mathsf{U}(S) \;=\; \text{Prob}\big[X \in S\big] \;=\; \frac{|S|}{n!}.$$

对每个子集 $S \subseteq \mathfrak{S}_n$, 可得 k 步以后我们的牌按照 S 中的某个置换排列的概率是

$$\begin{aligned}
\mathsf{Q}^{*k}(S) \;=\;& \text{Prob}[X_k \in S] \\
=\;& \sum_{j \leqslant k} \text{Prob}[X_k \in S \,\wedge\, T = j] \;+\; \text{Prob}[X_k \in S \,\wedge\, T > k] \\
=\;& \sum_{j \leqslant k} \mathsf{U}(S)\,\text{Prob}[T = j] \;+\; \text{Prob}[X_k \in S \,|\, T > k] \cdot \text{Prob}[T > k] \\
=\;& \mathsf{U}(S)\,(1 - \text{Prob}[T > k]) \;+\; \text{Prob}[X_k \in S \,|\, T > k] \cdot \text{Prob}[T > k] \\
=\;& \mathsf{U}(S) \;+\; \big(\text{Prob}[X_k \in S \,|\, T > k] - \mathsf{U}(S)\big) \cdot \text{Prob}[T > k].
\end{aligned}$$

由于

$$\text{Prob}[X_k \in S \,|\, T > k] \;-\; \mathsf{U}(S)$$

是两个概率的差, 绝对值至多是 1, 从而

$$|\mathsf{Q}^{*k}(S) - \mathsf{U}(S)| \;\leqslant\; \text{Prob}[T > k]. \qquad \square$$

这是我们完成关于顶牌随机插入式洗牌法分析的关键地方: 我们已经证明了下面这个为达到"接近随机"所需的洗牌数的一个上界.

定理 1. *设 $c \geqslant 0, k := \lceil n\log n + cn \rceil$, 且一副牌有 n 张. 则在进行了 k 次顶牌随机插入的洗牌后, 到均匀分布的变差距满足*

$$d(k) \; := \; \|\mathsf{Top}^{*k} - \mathsf{U}\| \; \leqslant \; e^{-c}.$$

容易验证, 如果顶牌随机插入的洗牌次数明显少于 $n\log n$, 变差距 $d(k)$ 保持较大. 这是因为较少次数的洗牌不足以破坏最底下那些牌的相对次序.

当然, 顶牌随机插入洗牌法效率极低 —— 根据我们定理中的界, 要想把一副 $n = 52$ 张卡片的牌混合好, 需要多于 $n\log n \approx 205$ 次顶牌随机插入. 因此我们现在把注意力转向一种有趣得多, 也现实得多的洗牌模型.



流插式洗牌法

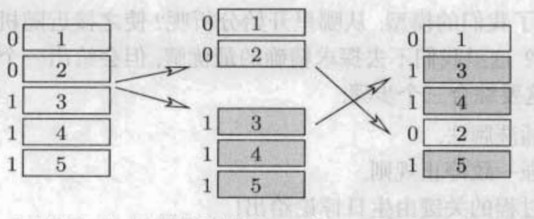
流插式洗牌

这是赌场庄家的操作方式: 他们拿起牌, 分成两部分, 然后互相交叉嵌入, 比方说从两半的底部按某种不规则的模式开始落下卡片.

流插仍旧只是把某些置换作用到牌上; 我们开始假设卡片从 1 到 n 标号, 其中 1 是顶卡. 流插洗牌确切对应着使得序列

$$(\pi(1), \pi(2), \cdots, \pi(n))$$

包含两个交错的增序列的置换 $\pi \in \mathfrak{S}_n$ (仅对单位置换是 1 个增序列), 故对 n 张卡片的牌共有 $2^n - n$ 个不同的流插.



事实上, 如果分摞使得上面的 t 张卡片在右手 $(0 \leqslant t \leqslant n)$, 其他的 $n-t$ 张卡片在左手, 则共有 $\binom{n}{t}$ 种方法来交错两手中的卡片, 都产生不同的置换 —— 除了对每个 t 都有一种可能来得到单位置换 (译者注: 此处及以下的两个递增子序列要求分别形如 $1, 2, \cdots, t$ 和 $t+1, \cdots, n$.).

现在还不清楚流插洗牌有怎样的概率分布, 由于业余与职业的庄家洗牌方式不同, 并没有唯一的答案. 尽管如此, 下面这个首先由 Edgar N. Gilbert 和 Claude Shannon 在 1955 年发展起来的模型 (当时是在传奇的贝尔实验室 "通讯数学" 部) 有几个优点:

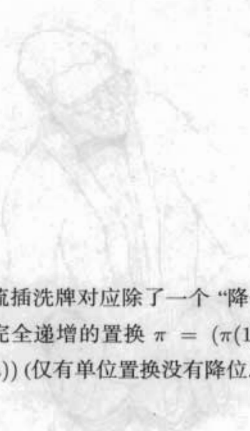
- 优雅, 简单, 看上去自然,
- 把业余爱好者洗牌的方式模拟得非常好,
- 便于分析.

以下是 $\mathfrak{S}_n$ 上概率分布 Rif 的三种等价描述:

1. $\mathsf{Rif} : \mathfrak{S}_n \longrightarrow \mathbb{R}$ 定义如下

$$\mathsf{Rif}(\pi) \ := \ \begin{cases} \frac{n+1}{2^n}, & 若 \pi = \mathrm{id}, \\ \frac{1}{2^n}, & 若 \pi 由两个递增子序列组成, \\ 0, & 其他情况. \end{cases}$$

2. 从牌中以 $\frac{1}{2^n}\binom{n}{t}$ 的概率拿掉 t 张卡片, 放在右手, 剩余的卡片放在左手. 现在, 当右边有 r 张卡片, 左边有 ℓ 张卡片时, 以 $\frac{r}{r+\ell}$ 的概率 "落" 右手的底牌, 同时以 $\frac{\ell}{r+\ell}$ 的概率落左手的底牌. 重复这一过程!
3. 逆洗是从牌中取一个子集的卡片, 拿出来, 再放到剩余卡片的上头 —— 保持两摞牌的相对次序. 这个动作是由所取的子集决定的: 以相同的概率取所有的子集.
   等价地, 给每张卡片随机、独立地以概率 $\frac{1}{2}$ 分配标号 "0" 或 "1", 再把标 "0" 的卡片移到顶部.



逆流插洗牌对应除了一个 "降位" 以外完全递增的置换 $\pi = (\pi(1), \cdots, \pi(n))$ (仅有单位置换没有降位.)

易见这些描述产生相同的概率分布. 关于 (1) $\Longleftrightarrow$ (3) 只需注意到当所有标 0 的卡片恰好取自所有标 1 的卡片的上方就得到单位置换.

以上定义了我们的模型. 从哪里开始分析呢? 使之接近随机需要多少次流插? 这里我们不去探求精确的最优解, 但会给出一个相当好的答案, 这要综合三个步骤:

(1) 分析逆流插洗牌法,
(2) 描述一个强一致停止规则,
(3) 证明分析过程的关键由生日悖论给出!

定理 2. *在一副 n 张卡片的牌上操作 k 次流插洗牌后, 到均匀分布的变差距满足*

$$\|\mathsf{Rif}^{*k} - \mathsf{U}\| \ \leqslant \ 1 - \prod_{i=1}^{n-1}\left(1 - \frac{i}{2^k}\right).$$

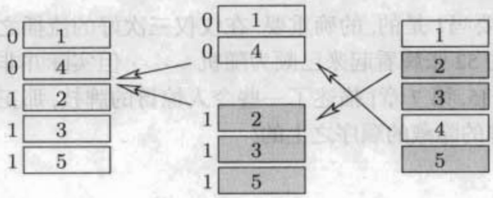
■ **证明.** (1) 我们事实上分析逆流插洗牌, 试图得出从初始分布到 (接近) 均匀有多快. 逆洗牌对应由 $\overline{\mathrm{Rif}}(\pi) := \mathrm{Rif}(\pi^{-1})$ 给出的概率分布.

每个置换有唯一逆的事实以及 $\mathrm{U}(\pi) = \mathrm{U}(\pi^{-1})$ 导致

$$\|\mathrm{Rif}^{*k} - \mathrm{U}\| = \|\overline{\mathrm{Rif}}^{*k} - \mathrm{U}\|.$$

(这是 Reeds 的逆引理!)

(2) 在每次逆流插洗牌中, 每张卡片被分配了数字 0 或 1:

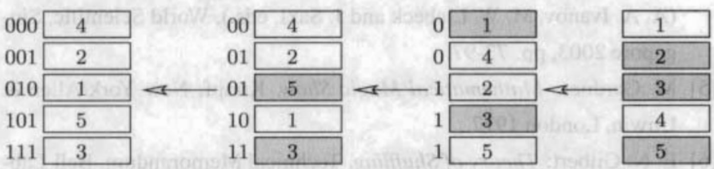


如果我们记下这些数字 —— 比方说写在卡片上 —— 那么 k 次逆流插之后, 每张卡片上有了一个 k 位的有序数字串. 我们的停止规则是:

"当所有卡片得到互异的数字串, 停."

此时, 牌中的卡片根据二元数字 $b_k b_{k-1} \cdots b_2 b_1$ 排序, 其中 b_i 是卡片在第 i 次逆流插洗牌中得到的数字. 由于这些数字完全随机、独立, 这个停止规则是强一致的!

下面的例子中有 $n = 5$ 张卡片, 需要做 $T = 3$ 次逆洗牌然后停止:



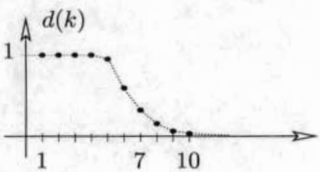
(3) 停止规则需要的时间 T 的分布由生日悖论确定, 取 $K = 2^k$: 把两张卡片放在一个盒子里, 当它们有相同的标签 $b_k b_{k-1} \cdots b_2 b_1 \in \{0,1\}^k$. 因此共有 $K = 2^k$ 个盒子, 而某个盒子含有多于 1 张卡片的概率是

$$\mathrm{Prob}[T > k] = 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{2^k}\right).$$

如前面所见, 这给出了变差距 $\|\mathrm{Rif}^{*k} - \mathrm{U}\| = \|\overline{\mathrm{Rif}}^{*k} - \mathrm{U}\|$ 的上界. □

k	$d(k)$
1	1.000
2	1.000
3	1.000
4	1.000
5	0.952
6	0.614
7	0.334
8	0.167
9	0.085
10	0.043

根据 [2], k 次流插洗牌后的变差距



那么我们需要洗多少次牌呢？当 n 比较大时大约需要 $k = 2\log_2(n)$ 次洗牌. 事实上, 对某个 $c \geqslant 1$, 置 $k := 2\log_2(cn)$, 我们发现 (用一点微积分) $P[T > k] \approx 1 - e^{-\frac{1}{2c^2}} \approx \frac{1}{2c^2}$.

具体说, 当有 $n = 52$ 张卡片时, 通过定理 2 中的上界算得 $d(10) \leqslant 0.73$, $d(12) \leqslant 0.28$, $d(14) \leqslant 0.08$, 所以 $k = 12$ 在实践意义上应该是 “足够随机” 了. 但我们 “在实践中” 并不洗 12 次牌, 因为更细致的分析表明那么多次并不真的必要 (结果在边栏给出). 对流插洗牌的分析是当前活跃的关于什么是 “足够随机” 的正确度量的讨论的一部分. Diaconis [4] 提供了关于最新进展的一个导引.

事实上, 这重要吗? 是的, 的确重要: 在仅仅三次好的流插之后一副重新排序了的 52 张牌看起来已颇为随机 …… 但实际并非如此. Martin Gardner [5, 第 7 章] 描述了一些令人惊讶的牌技, 那正是建立在这样一副牌的隐藏的顺序之上的!

参考文献

[1] D. Aldous & P. Diaconis: *Shuffling cards and stopping times,* Amer. Math. Monthly **93** (1986), 333-348.

[2] D. Bayer & P. Diaconis: *Trailing the dovetail shuffle to its lair,* Annals Applied Probability **2** (1992), 294-313.

[3] E. Behrends: *Introduction to Markov Chains,* Vieweg, Braunschweig /Wiesbaden 2000.

[4] P. Diaconis: *Mathematical developments from the analysis of riffle shuffling,* in:"Groups, Combinatorics and Geometry. Durham 2001" (A. A. Ivanov, M. W. Liebeck and J. Saxl, eds.), World Scientific, Singapore 2003, pp. 73-97.

[5] M. Gardner: *Mathematical Magic Show,* Knopf, New York/Allen & Unwin, London 1977.

[6] E. N. Gilbert: *Theory of Shuffling,* Technical Memorandum, Bell Laboratories, Murray Hill NJ, 1955.



足够随机了吗?

而路径族 P_n 的载重则是各条路径净重的乘积:



格路径与行列式

第 25 章

数学的精华部分是证明定理. 于是, 这就成了数学家们要做的事: 他们证明定理. 但是说实话, 他们真正想证明的, 一生中一次就够了的, 是引理, 例如 Fatou 在分析中的那个引理, 数论中的高斯引理, 或者组合数学中的 Burnside-Frobenius 引理.

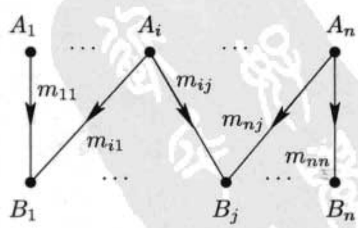
那什么样的数学命题是真正的引理呢? 首先, 它应该适用于比较广泛的情形, 甚至是看起来无关的问题. 其次, 这个命题应该一看上去就是显然的. 读者的反应也许正是有点嫉妒: 为什么我没有先注意到呢? 第三, 在审美的层面上, 引理 —— 包括其证明 —— 应该是美丽的!

在本章中, 我们看这样一个数学推理的杰作, 首先出现在 Bernt Lindström 的 1972 年文章中的计数引理. 这个结果当时没怎么受到重视, 直到 1985 年才瞬间成为经典: 那年 Ira Gessel 和 Gerard Viennot 再次发现它, 且在一篇精彩文章中展示了这个引理如何可以在多种困难的组合计数问题上应用.

出发点是矩阵行列式的通常置换表示. 设 $M = (m_{ij})$ 是实的 $n \times n$- 矩阵, 则

$$\det M \;=\; \sum_{\sigma} \operatorname{sign}\sigma \; m_{1\sigma(1)}\, m_{2\sigma(2)} \cdots m_{n\sigma(n)}, \qquad (1)$$

其中 σ 遍历所有的 $\{1, 2, \cdots, n\}$ 上的置换, σ 的符号 $\operatorname{sign}\sigma$ 是 1 还是 -1, 取决于 σ 是偶数个还是奇数个轮换的乘积.



现在我们转向图, 具体说是有向加权二部图. 令顶点 $A_1, \cdots, A_n$ 代表 M 的行, $B_1, \cdots, B_n$ 代表列. 对每个对 i 和 j, 画一个从 A_i 到 B_j 的箭头, 赋以权重 m_{ij}, 如图所示.

就图而言, 公式 (1) 有如下解释:

- 左端是*路径矩阵* M 的行列式, 其中矩阵的 (i, j)- 元素是从 A_i 到 B_j 的 (唯一) 有向路径的*权重*.
- 右端是从 $\mathcal{A} = \{A_1, \cdots, A_n\}$ 到 $\mathcal{B} = \{B_1, \cdots, B_n\}$ 的所有*顶点不交路径族* 的权重 (带符号) 和. 这样一个族 $\mathcal{P}_\sigma$ 形如

$$A_1 \to B_{\sigma(1)}, \;\; \cdots \;\; , A_n \to B_{\sigma(n)},$$

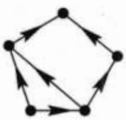
而路径族 $\mathcal{P}_\sigma$ 的权重则是各条路径权重的乘积:

$$w(\mathcal{P}_\sigma) \;=\; w(A_1 \to B_{\sigma(1)}) \;\cdots\; w(A_n \to B_{\sigma(n)}).$$

在这种解释下公式 (1) 读作

$$\det M \;=\; \sum_\sigma \operatorname{sign}\sigma\, w(\mathcal{P}_\sigma).$$

那么 Gessel 和 Viennot 的结果是什么呢? 它是公式 (1) 从二部图到任意的图的自然推广. 正是这一步使得引理应用广泛, 此外, 它的证明惊人的简洁和高雅.



一个无圈有向图

让我们先介绍一些必要的概念. 给定有限、有向但无圈的图 $G = (V, E)$, 这里无圈表示 G 里没有有向的圈. 特别地, 在任意两个顶点 A 和 B 之间仅有有限多个有向路径, 这里我们允许长度为 0 的平凡路径 $A \to A$. 每条边 e 带一个权重 $w(e)$. 若 P 是从 A 到 B 的有向路径, 简记为 $P : A \to B$, 则定义 P 的权重 为

$$w(P) \;:=\; \prod_{e\in P} w(e),$$

而当 P 是长为 0 的路径时, 规定 $w(P) = 1$.

现在令 $\mathcal{A} = \{A_1, \cdots, A_n\}$ 及 $\mathcal{B} = \{B_1, \cdots, B_n\}$ 为两组 n 个顶点的集合, 其中 $\mathcal{A}$ 和 $\mathcal{B}$ 不一定不交. 我们为 $\mathcal{A}$ 和 $\mathcal{B}$ 指定一个路径矩阵 $M = (m_{ij})$ 使得

$$m_{ij} \;:=\; \sum_{P:A_i\to B_j} w(P).$$

从 $\mathcal{A}$ 到 $\mathcal{B}$ 的路径族 $\mathcal{P}$ 包含一个置换 σ 及 n 个路径 $P_i : A_i \to B_{\sigma(i)}$, 其中 $i = 1, \cdots, n$; 记 $\operatorname{sign}\mathcal{P} = \operatorname{sign}\sigma$. $\mathcal{P}$ 的权重是各路径的权重积

$$w(\mathcal{P}) \;=\; \prod_{i=1}^{n} w(P_i), \tag{2}$$

即该路径族所含的所有边的权重之积.

最后, 称路径族 $\mathcal{P} = (P_1, \cdots, P_n)$ 是顶点不交的, 若 $\mathcal{P}$ 里的路径是两两顶点不交的.

引理. 设 $G = (V, E)$ 是有限加权无圈的有向图, $\mathcal{A} = \{A_1, \cdots, A_n\}$ 和 $\mathcal{B} = \{B_1, \cdots, B_n\}$ 是两组基数为 n 的顶点集, 且 M 是从 $\mathcal{A}$ 到 $\mathcal{B}$ 的路径矩阵, 则

$$\det M \;=\; \sum_{\substack{\mathcal{P}\text{是顶点不}\\ \text{交的路径族}}} \operatorname{sign}\mathcal{P}\, w(\mathcal{P}). \tag{3}$$

■ **证明.** $\det M$ 中一个典型项形如 $\text{sign}\sigma m_{1\sigma(1)}\cdots m_{n\sigma(n)}$, 也可写为

$$\text{sign}\sigma\Big(\sum_{P_1:A_1\to B_{\sigma(1)}} w(P_1)\Big)\cdots\Big(\sum_{P_n:A_n\to B_{\sigma(n)}} w(P_n)\Big).$$

对 σ 求和立即从 (2) 得

$$\det M = \sum_{\mathcal{P}} \text{sign}\,\mathcal{P} w(\mathcal{P}),$$

这里 $\mathcal{P}$ 的取值范围是从 $\mathcal{A}$ 到 $\mathcal{B}$ 的所有 路径族 (无论顶点不交与否). 所以, 为得到 (3) 我们只需证明

$$\sum_{\mathcal{P}\in N} \text{sign}\,\mathcal{P} w(\mathcal{P}) = 0, \qquad (4)$$

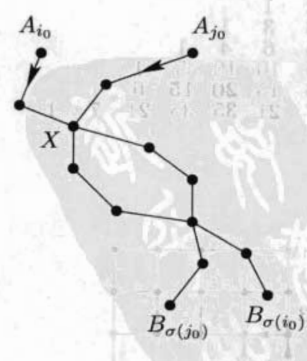
其中 N 是所有非顶点不交的路径族的集合. 这由一个极美的论证来实现. 为此我们展示一个对合 $\pi: N\to N$ (没有不动点的) 使得对 $\mathcal{P}$ 和 $\pi\mathcal{P}$ 恒有

$$w(\pi\mathcal{P}) = w(\mathcal{P}) \quad 及 \quad \text{sign}\,\pi\mathcal{P} = -\text{sign}\,\mathcal{P}.$$

显然, 这将推出 (4), 从而引理中的 (3) 成立.

对合 π 的定义是极自然的. 设 $\mathcal{P}\in N$ 由路径 $P_i: A_i\to B_{\sigma(i)}$ 组成. 根据定义, 某对路径会相交:

- 令 i_0 为使得 P_{i_0} 与其他路径共有顶点的最小的指标.
- 令 X 为 P_{i_0} 上第一个与其他路径共有的顶点.
- 令 j_0 为最小的满足 $j_0 > i_0$ 且使得 P_{j_0} 与 P_{i_0} 共有 X 为顶点的指标.



现在构造新的族 $\pi\mathcal{P} = (P'_1,\cdots,P'_n)$ 如下:

- 置 $P'_k = P_k$, 对所有的 $k\neq i_0, j_0$.
- 新的路径 P'_{i_0} 沿着 P_{i_0} 从 A_{i_0} 到 X, 但接着沿着 P_{j_0} 走到 $B_{\sigma(j_0)}$. 类似地, P'_{j_0} 沿着 P_{j_0} 从 A_{j_0} 到 X, 然后沿着 P_{i_0} 到 $B_{\sigma(i_0)}$.

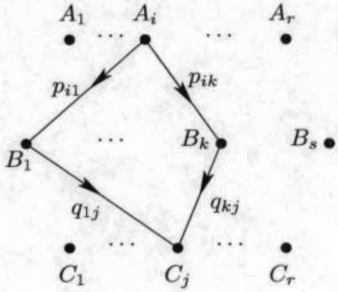
显然有 $\pi(\pi\mathcal{P}) = \mathcal{P}$, 因为指标 i_0、顶点 X 及指标 j_0 都没有变. 换言之, 应用 π 两次我们就回到原来的路径 P_i. 接着, 由于 $\pi\mathcal{P}$ 与 $\mathcal{P}$ 有完全相同的边, 自然有 $w(\pi\mathcal{P}) = w(\mathcal{P})$. 最后, 由于新的置换 σ' 可以通过原置换 σ 乘以对换 (i_0, j_0) 得到, 我们发现 $\text{sign}\,\pi\mathcal{P} = -\text{sign}\,\mathcal{P}$, 证毕. □

Gessel-Viennot 引理可被用来推导出行列式的所有基本性质, 这只需观察合适的图. 让我们考虑一个特别显著的例子: Binet-Cauchy 公式, 它给出了行列式乘法准则的一个非常有用的推广.

定理. 设 P 为一个 $(r\times s)$- 矩阵, Q 为一个 $(s\times r)$- 矩阵, 其中 $r\leqslant s$, 则

$$\det(PQ) \;=\; \sum_{\mathcal{Z}}(\det P_{\mathcal{Z}})(\det Q_{\mathcal{Z}}),$$

其中 $P_{\mathcal{Z}}$ 是 P 的列集合为 $\mathcal{Z}$ 的 $(r\times r)$- 子矩阵, $Q_{\mathcal{Z}}$ 是 Q 的行对应取自 $\mathcal{Z}$ 的 $(r\times r)$- 子矩阵.



■ **证明.** 如前, 令 $\mathcal{A}$ 和 $\mathcal{B}$ 上的二部图对应 P, 类似地, $\mathcal{B}$ 和 $\mathcal{C}$ 上的二部图对应 Q. 现在考虑边图所示的合在一起的拼接图, 观察到从 $\mathcal{A}$ 到 $\mathcal{C}$ 的路径矩阵 M 的 (i,j)- 处元素 m_{ij} 恰为 $m_{ij}=\sum_k p_{ik}q_{kj}$, 故 $M=PQ$.

由于拼接图中由 $\mathcal{A}$ 到 $\mathcal{C}$ 的顶点不交路径族对应从 $\mathcal{A}$ 到 $\mathcal{Z}$ 及从 $\mathcal{Z}$ 到 $\mathcal{C}$ 的族对, 注意 $(\sigma\tau)=(\operatorname{sign}\sigma)\,(\operatorname{sign}\tau)$, 由引理立有结论. □

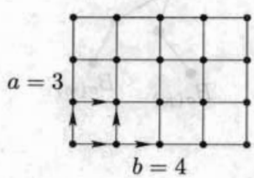
从 Gessel-Viennot 引理发源, 我们可以得到一大批将行列式与计数性质联系在一起的结果. 诀窍都相同: 把矩阵 M 看作路径矩阵, 试图计算 (3) 的右端. 作为示范我们考虑当年 Gessel 和 Viennot 研究的初始问题, 是它引出了他们的引理:

> 设 $a_1<a_2<\cdots<a_n$ 与 $b_1<b_2<\cdots<b_n$ 是两组自然数. 我们希望计算矩阵 $M=(m_{ij})$ 的行列式, 其中 m_{ij} 是二项式系数 $\binom{a_i}{b_j}$.

1
1 1
1 2 1
1 **3** 3 **1**
1 **4** 6 **4** **1**
1 5 10 10 5 1
1 **6** 15 **20** **15** 6 1
1 7 21 35 35 21 7 1

换句话说, Gessel 和 Viennot 看的是 Pascal 三角形上的任意方阵的行列式, 例如边栏上示例的 Pascal 三角形里以黑体字标出的元素组成的矩阵

$$\det\begin{pmatrix}\binom{3}{1} & \binom{3}{3} & \binom{3}{4}\\ \binom{4}{1} & \binom{4}{3} & \binom{4}{4}\\ \binom{6}{1} & \binom{6}{3} & \binom{6}{4}\end{pmatrix} \;=\; \det\begin{pmatrix}3 & 1 & 0\\ 4 & 4 & 1\\ 6 & 20 & 15\end{pmatrix}.$$

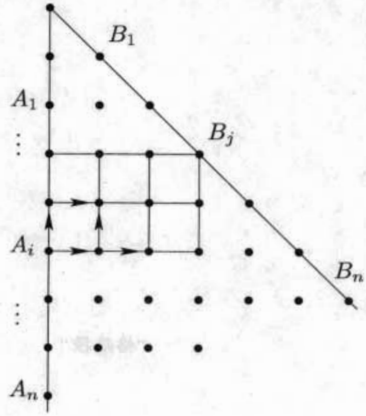


在解决问题之前我们回忆一个广为人知的结果, 它把二项式系数和格路径联系起来. 如边图所示, 考虑 $a\times b$ 的格子. 那么当只允许向上 (北) 的和向右 (东) 的步子, 从左下角到右上角的路径总数为 $\binom{a+b}{a}$.

证明很容易: 每条路径是一个由 b 个 "东 (E)" 与 a 个 "北 (N)" 步子组成的任意序列, 故可编码为由 $a+b$ 个字母组成的序列形如

NENEEEN, 其中有 a 个 N 和 b 个 E. 这种字符串的个数正是从 $a+b$ 个位置里选择 a 个留给字母 N 的方法数, 也就是 $\binom{a+b}{a}=\binom{a+b}{b}$.

现在看边上的图, A_i 置于点 $(0,-a_i)$ 处, B_j 则放在 $(b_j,-b_j)$ 处. 这个网格上从 A_i 到 B_j 且只用往北和往东的步子的路径总数, 如前所证是 $\binom{b_j+(a_i-b_j)}{b_j}=\binom{a_i}{b_j}$. 换句话说, 二项式系数的矩阵 M 正是有向网格图上从 $\mathcal{A}$ 到 $\mathcal{B}$ 的路径矩阵, 这里所有的边赋以权重 1, 且所有的边指向北或东. 因此, 为计算 $\det M$ 我们可以应用 Gessel-Viennot 引理. 稍加思考即知: 每个从 $\mathcal{A}$ 到 $\mathcal{B}$ 的顶点不交路径族 $\mathcal{P}$ 由所有的路径 $P_i: A_i\to B_i$ 组成. 于是唯一出现的置换是单位置换, 其符号 $=1$, 从而我们得到优美结果

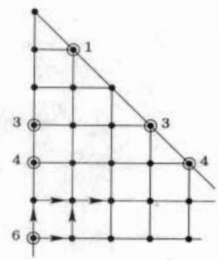


$$\det\left(\binom{a_i}{b_j}\right) \;=\; \text{从 }\mathcal{A}\text{到 }\mathcal{B}\text{ 的顶点不交路径族的总数.}$$

特别地, 由于等式的右端是个计数的结果, 从而表明 $\det M$ 非负这个极不明显的事实. 更进一步, 由 Gessel-Viennot 引理可得 $\det M=0$ 当且仅当对某个 i 有 $a_i<b_i$.

就先前的小小例子来说,

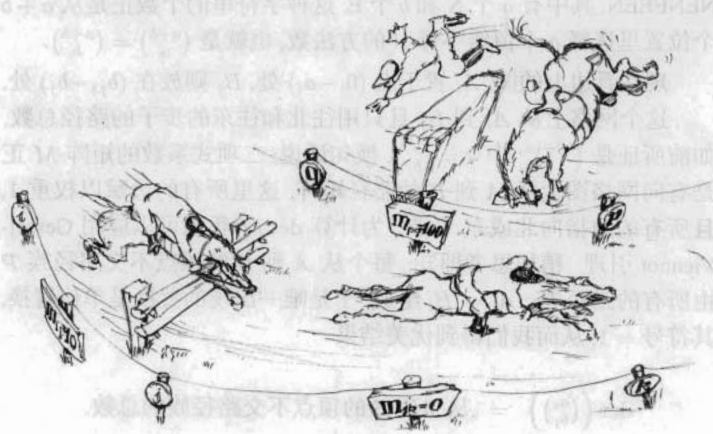
$$\det\begin{pmatrix}\binom{3}{1} & \binom{3}{3} & \binom{3}{4}\\ \binom{4}{1} & \binom{4}{3} & \binom{4}{4}\\ \binom{6}{1} & \binom{6}{3} & \binom{6}{4}\end{pmatrix} = \text{右图中的顶点不交路径族的总数:}$$



参考文献

[1] I. M. Gessel & G. Viennot: *Binomial determinants, paths, and hook length formulae,* Advances in Math. **58** (1985), 300-321.

[2] B. Lindström: *On the vector representation of induced matroids,* Bulletin. London Math. Soc. **5** (1973), 85-90.



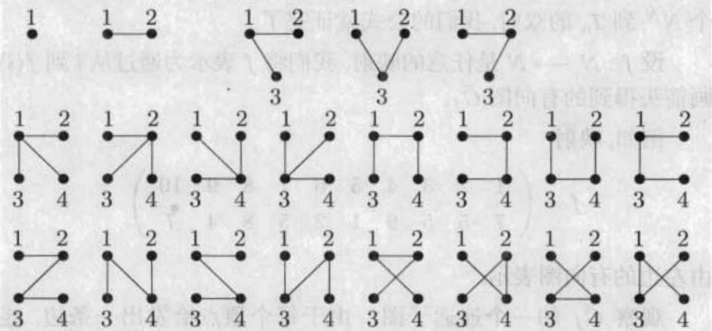
“格路径”

关于树计数的 Cayley 公式 第 26 章

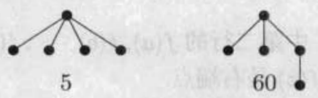


Arthur Cayley

计数组合学中最美的公式之一是关于带标记的树的数目. 考虑集合 $N = \{1, 2, \cdots, n\}$, 在这个顶点集上可以形成多少棵不同的树? 用 T_n 表示这个数. "手工" 计数表明 $T_1 = 1, T_2 = 1, T_3 = 3, T_4 = 16$, 这些树见下表:



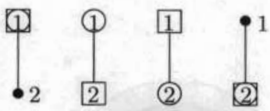
注意我们考虑的是标记树, 所以尽管在图同构的意义下仅有一棵阶为 3 的树, 通过将中间的顶点表为 1, 2 或 3 一共得到 3 棵不同的标记树. 当 $n = 5$ 时有 3 棵非同构的树:



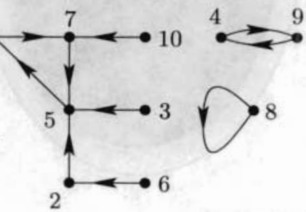
对第一棵树显然有 5 种标记方式, 第二、第三棵树则各有 $\frac{5!}{2} = 60$ 种标记, 故得 $T_5 = 125$. 这应已足以做出猜想 $T_n = n^{n-2}$, 这正是 Cayley 的结论.

定理. *在 n 个顶点上共有 n^{n-2} 棵不同的标记树.*

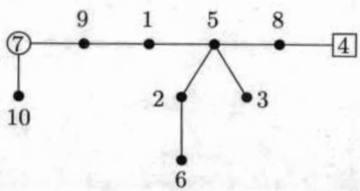
这个美丽的公式产生了众多优美的证明, 它们依靠种种组合与代数的技巧. 在展示至今最美的那个之前, 我们先概述其中的三个证明.



$\mathcal{T}_2$ 中的 4 棵树



$\vec{G}_f$



■ **第一个证明 (双射法).** 经典的和最直接的方法是找一个从所有 n 个顶点上的树到另一个已知基数为 n^{n-2} 的集合的双射. 自然, 所有满足 $1 \leqslant a_i \leqslant n$ 的有序数列 $(a_1, \cdots, a_{n-2})$ 映入脑海. 因此我们希望将每棵树 T 都由一个序列 $(a_1, \cdots, a_{n-2})$ 唯一地编码. 这样的一个码是 Prüfer 发现的, 在大多数图论的书中都找得到.

这里我们想要讨论另一个双射证明, 这归功于 Joyal, 名气不大但是同样的优雅和简洁. 为此, 我们不仅考虑 $N = \{1, \cdots, n\}$ 上的树 t, 而且还加两个特殊的顶点: *左端点* $\bigcirc$ 与*右端点* $\square$, 两者可能重合. 令 $\mathcal{T}_n = \{(t; \bigcirc, \square)\}$ 表示这个新的集合; 那么显然 $|\mathcal{T}_n| = n^2 T_n$.

于是我们的目标是证明 $|\mathcal{T}_n| = n^n$. 现在有一个集合的基数众所周知是 n^n, 那就是从 N 到 N 的所有映射 N^N. 因此如果找到一个 N^N 到 $\mathcal{T}_n$ 的双射, 我们的公式就证完了.

设 $f: N \longrightarrow N$ 是任意的映射. 我们将 f 表示为通过从 i 到 $f(i)$ 画箭头得到的有向图 $\vec{G}_f$.

例如, 映射

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 5 & 9 & 1 & 2 & 5 & 8 & 4 & 7 \end{pmatrix}$$

由左边的有向图表示.

观察 $\vec{G}_f$ 的一个连通子图. 由于每个顶点恰发出一条边, 连通子图含有同样多的顶点数和边数, 从而恰包含一条有向圈. 令 $M \subseteq N$ 为所有这些圈的顶点集合. 略加思索就知道 M 是唯一的 N 的极大子集满足 f 在 M 上的限制是 M 上的双射. 记 $f|_M = \begin{pmatrix} a & b & \cdots & z \\ f(a) & f(b) & \cdots & f(z) \end{pmatrix}$, 其中第一行的数字 $a, b, \cdots, z$ 按自然序列出现. 这给了我们一个 M 中第二行的 $f(a), f(b), \cdots, f(z)$ 的排序. 现在 $f(a)$ 就是左端点, 而 $f(z)$ 是右端点.

对应映射 f 的树 t 构造如下: 按顺序把 $f(a), \cdots, f(z)$ 画成从 $f(a)$ 到 $f(z)$ 的路, 将剩余的顶点按照 $\vec{G}_f$ 中的方式添加上去 (去掉箭头).

在上面的例子中, 我们得到 $M = \{1, 4, 5, 7, 8, 9\}$,

$$f|_M = \begin{pmatrix} 1 & 4 & 5 & 7 & 8 & 9 \\ 7 & 9 & 1 & 5 & 8 & 4 \end{pmatrix}$$

以及边白上画出的树 t.

马上可以将对应逆过去: 给定树 t, 看从左端点到右端点的唯一

的路 P. 这给了我们集合 M 和映射 $f|_M$. 剩下的对应 $i \to f(i)$ 由从 i 到 P 的唯一路径决定. □

■ **第二个证明 (线性代数法).** 可以把 T_n 看作完全图 K_n 的生成树的个数. 现在让我们看 $V = \{1, 2, \cdots, n\}$ 上一个任意的简单连通图 G, 用 $t(G)$ 表示其生成树的个数; 于是 $T_n = t(K_n)$. 下面的著名结果是 Kirchhoff 的*矩阵树定理* (见 [1]). 考虑 G 的关联矩阵 $B = (b_{ie})$, 其行用 V 标记, 列用 E 标记, 由 $i \in e$ 或 $i \notin e$ 记 $b_{ie} = 1$ 或 0. 注意因为 G 是连通的, $|E| \geqslant n-1$. 在每一列将两个 1 中的任一个换成 -1 (这相当于给 G 定向), 记新得到的矩阵为 C. 则 $M = CC^T$ 是对称的 $(n \times n)$- 矩阵, 且主对角线上是顶点的度数 $d_1, \cdots, d_n$.

性质. *对所有的 $i = 1, \cdots, n$, 有 $t(G) = \det M_{ii}$, 这里 M_{ii} 是 M 中去掉第 i 行及第 i 列得到的矩阵.*

■ **证明.** 证明的关键是前一章证过的 Binet-Cauchy 定理: 若 P 是 $(r \times s)$- 矩阵, Q 是 $(s \times r)$- 矩阵, $r \leqslant s$, 则 $\det(PQ)$ 等于所有对应的 $(r \times r)$- 子矩阵行列式的乘积之和, 这里 "对应" 意味着取相同指标集的 P 的 r 列和 Q 的 r 行.

对 M_{ii} 这表明

$$\det M_{ii} = \sum\nolimits_N \det N \cdot \det N^T = \sum\nolimits_N (\det N)^2,$$

其中 N 取遍所有 $C\backslash\{第\ i行\}$ 的 $(n-1) \times (n-1)$ 子矩阵. N 的这 $n-1$ 列对应 G 的 n 个顶点上的 $n-1$ 条边的子图, 故剩下的只须证

$$\det N = \begin{cases} \pm 1 & 当这些边生成一棵树 \\ 0 & 否则. \end{cases}$$

假设某 $n-1$ 条边不生成树, 则存在不含 i 的连通子块. 由于这个块对应的所有行加起来是 0 向量, 它们线性相关, 因此 $\det N = 0$.

现在假设 N 的列生成了树, 则存在度数为 1 的顶点$j_1 \neq i$; 设 e_1 是其相邻的边. 删除 j_1, e_1, 我们得到一棵有 $n-2$ 条边的树. 仍旧, 有度数为 1 的顶点 $j_2 \neq i$ 和边 e_2 相邻. 继续下去直到决定 $j_1, j_2, \cdots, j_{n-1}$ 及 $e_1, e_2, \cdots, e_{n-1}$ 满足 $j_i \in e_i$. 现在置换行和列使得 j_k 在第 k 行, e_k 在第 k 列. 由构造知当 $k < \ell$ 有 $j_k \notin e_\ell$, 所以新的矩阵 N' 是下三角的, 且所有主对角线上的元素等于 ± 1. 因此 $\det N = \pm \det N' = \pm 1$, 证毕. □



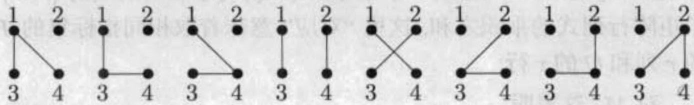
"一个非标准的计数树的方法: 每棵树上放只猫, 遛狗经过, 计数犬吠的次数."

对 $G = K_n$ 的特殊情况, 显然有

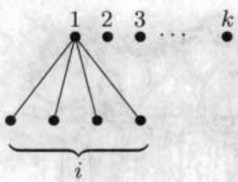
$$M_{ii} = \begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix}.$$

简单的计算显示 $\det M_{ii} = n^{n-2}$.

■ **第三个证明 (递归法).** 另一个计数组合学中的经典方法是建立递归关系, 再用归纳法解决之. 下面的思想本质上归功于 Riordan 和 Rényi. 为找到合适的递归, 我们考虑一个更一般的问题 (这在 Cayley 的文章中已经出现了). 令 A 为顶点集合的任意 k- 子集. 用 $T_{n,k}$ 表示 $\{1, \cdots, n\}$ 上包含 k 个树, 且 A 中的顶点都在不同树里的 (标记) 森林的个数. 显然, 集合 A 的选取无关紧要, 要紧的是其基数 k. 注意到 $T_{n,1} = T_n$.



例如, 当 $A = \{1, 2\}$ 时 $T_{4,2} = 8$.



设 $A = \{1, 2, \cdots, k\}$, 考虑如边图所示的森林 F, 其顶点 1 与 i 个顶点相邻. 删去 1, 则它的 i 个邻居与 $2, \cdots, k$ 在一个有 $k-1+i$ 棵树的森林里面, 且这些顶点都在不同的连通块中. 先选定 1 的 i 个邻居, 再确定 $F\backslash 1$, 然后可以 (重新) 构造出 F. 这表明对任意的 $n \geqslant k \geqslant 1$, 有

$$T_{n,k} = \sum_{i=0}^{n-k} \binom{n-k}{i} T_{n-1,k-1+i}. \tag{1}$$

以上对于 $n > 0$, 置 $T_{0,0} = 1$, 及 $T_{n,0} = 0$. 注意为保证 $T_{n,n} = 1$, $T_{0,0} = 1$ 是必要的.

命题. 我们有

$$T_{n,k} = k\, n^{n-k-1}, \tag{2}$$

从而特别地,

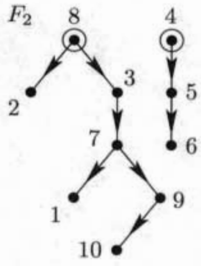
$$T_{n,1} = T_n = n^{n-2}.$$

■ **证明.** 由 (1), 利用归纳, 我们发现

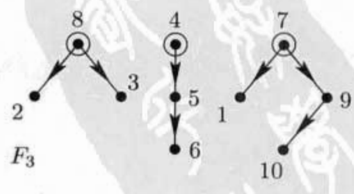
$$\begin{aligned} T_{n,k} &= \sum_{i=0}^{n-k}\binom{n-k}{i}(k-1+i)(n-1)^{n-1-k-i} \quad (i \to n-k-i) \\ &= \sum_{i=0}^{n-k}\binom{n-k}{i}(n-1-i)(n-1)^{i-1} \\ &= \sum_{i=0}^{n-k}\binom{n-k}{i}(n-1)^{i} - \sum_{i=1}^{n-k}\binom{n-k}{i} i(n-1)^{i-1} \\ &= n^{n-k} - (n-k)\sum_{i=1}^{n-k}\binom{n-1-k}{i-1}(n-1)^{i-1} \\ &= n^{n-k} - (n-k)\sum_{i=0}^{n-1-k}\binom{n-1-k}{i}(n-1)^{i} \\ &= n^{n-k} - (n-k)n^{n-1-k} = k n^{n-1-k}. \end{aligned}$$ □

■ **第四个证明 (双计数法).** 以下的精彩思想归功于 Jim Pitman, 他在没有用归纳或双射的情况下给出了 Cayley 公式及其推广 (2) —— 仅凭在两个方向进行聪明地计数.

$\{1, \cdots, n\}$ 上的有根森林是在每个分块树上选定一个根的森林. 令 $\mathcal{F}_{n,k}$ 表示由 k 棵有根树组成的所有有根森林的集合, 则 $\mathcal{F}_{n,1}$ 是所有有根树的集合.



F_2 包含 F_3



注意 $|\mathcal{F}_{n,1}| = nT_n$, 因为每棵树有 n 个可以选择的根. 现在把 $F_{n,k} \in \mathcal{F}_{n,k}$ 看成有向图, 所有的边从根开始指向远处. 称森林 F 包含另一个森林 F', 若 F 在有向图的意义上包含 F'. 显然, 若 F 真包含 F', 则 F 有比 F' 少的分块. 两个这样的森林如图所示, 根放在顶部.

下面是关键的思想. 称森林序列 $F_1, \cdots, F_k$ 为改进序列, 若 $F_i \in \mathcal{F}_{n,i}$ 且对所有的 i 有 F_i 包含 F_{i+1}.

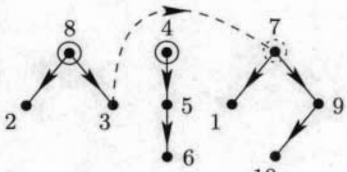
设 F_k 是 $\mathcal{F}_{n,k}$ 中选定的树, 用

- $N(F_k)$ 表示包含 F_k 的有根树的数目,
- $N^*(F_k)$ 表示以 F_k 结束的改进序列的数目.

对 $N^*(F_k)$ 双计数, 先从树开始再从 F_k 开始. 假设 $F_1 \in \mathcal{F}_{n,1}$ 包含 F_k. 由于我们可以按任意的顺序删去 $F_1 \backslash F_k$ 的 $k-1$ 条边来得到从 F_1 到 F_k 的改进序列, 我们发现

$$N^*(F_k) = N(F_k)\,(k-1)!. \tag{3}$$

现在从另一头出发. 为从 F_k 得到 F_{k-1}, 必须加上一条有向边,



$F_3 \longrightarrow F_2$

这条边应该是从任意的顶点 a 出发指向不含 a 的 $k-1$ 棵树的任意某棵之根的. (见边图所示, 我们通过增加边 $3 \bullet\!\!\longrightarrow\!\!\bullet 7$ 由 F_3 得到了 F_2).于是我们有 $n(k-1)$ 个选择. 类似地, 对 F_{k-1} 可以从某个顶点 b 朝不含 b 的 $k-2$ 棵树的任意某棵之根增加有向边. 对此有 $n(k-2)$ 个选择. 继续下去, 我们得到

$$N^*(F_k) \;=\; n^{k-1}(k-1)!, \tag{4}$$

这和 (3) 合在一起给出了意想不到的简单关系

$$N(F_k) = n^{k-1} \qquad \text{对任意} F_k \in \mathcal{F}_{n,k}.$$

当 $k=n$, F_n 仅仅由 n 个孤立顶点组成. 因此 $N(F_n)$ 计数所有的有根树的数目, 于是 $|\mathcal{F}_{n,1}| = n^{n-1}$, 从而得到 Cayley 公式. □

而我们甚至从这证明中得到更多. 公式 (4) 表明对于 $k=n$:

$$\#\{\text{改进序列 } (F_1, F_2, \cdots, F_n)\} \;=\; n^{n-1}(n-1)!. \tag{5}$$

对 $F_k \in \mathcal{F}_{n,k}$, 令 $N^{**}(F_k)$ 表示第 k 项为 F_k 的改进序列 $F_1, \cdots, F_n$ 的数目. 显然, 这等于 $N^*(F_k)$ 乘以选择 $(F_{k+1}, \cdots, F_n)$ 的方式的数目. 而后者是 $(n-k)!$, 因为我们可以按任意的方式删掉 F_k 中的 $n-k$ 条边. 这样

$$N^{**}(F_k) \;=\; N^*(F_k)(n-k)! \;=\; n^{k-1}(k-1)!(n-k)!. \tag{6}$$

由于这个数不依赖 F_k 的选择, (6) 除 (5) 给出了含有 k 棵树的有根森林的数目:

$$|\mathcal{F}_{n,k}| \;=\; \frac{n^{n-1}(n-1)!}{n^{k-1}(k-1)!(n-k)!} \;=\; \binom{n}{k} k\, n^{n-1-k}.$$

因为有 $\binom{n}{k}$ 种方式选择 k 个根, 我们不用归纳而再一次证明了公式 $T_{n,k} = kn^{n-k-1}$.

让我们用一段历史轶事来结束本章. Cayley 在 1889 年的文章已经被 Carl W. Borchardt 在 1860 年预见到了, 这个事实为 Cayley 本人所承认. 一个等价的结果甚至出现得更早, 那是在 1857 年 James J. Sylvester 的一篇文章里, 见 [2, 第 3 章]. Cayley 论文的新意在于使用了图论中的术语; 从那以后, 这个定理就被冠以他的名字.

参考文献

[1] M. Aigner: *Combinatorial Theory,* Springer-Verlag, Berlin Heidelberg New York 1979; Reprint 1997.

[2] N. L. Biggs, E. K. Lloyd & R. J. Wilson: *Graph Theory 1736-1936,* Clarendon Press, Oxford 1976.

[3] A. Cayley: *A theorem on trees,* Quart. J. Pure Appl. Math. **23** (1889), 376-378; Collected Mathematical Papers Vol. 13, Cambridge University Press 1897, 26-28.

[4] A. Joyal: *Une théorie combinatoire des séries formelles,* Advances in Math. **42** (1981), 1-82.

[5] J. Pitman: *Coalescent random forests,* J. Combinatorial Theory, Ser. A **85** (1999), 165-193.

[6] H. Prüfer: *Neuer Beweis eines Satzes über Permutationen,* Archiv der Math. u. Physik (3) **27** (1918), 142-144.

[7] A. Rényi: *Some remarks on the theory of trees.* MTA Mat. Kut. Inst. Kozl. (Publ. math. Inst. Hungar. Acad. Sci.) **4** (1959), 73-85; Selected Papers Vol. 2, Akadémiai Kiadó, Budapest 1976, 363-374.

[8] J. Riordan: *Forests of labeled trees,* J. Combinatorial Theory **5** (1968), 90-103.

参考文献

[1] M. Aigner: *Combinatorial Theory*, Springer-Verlag, Berlin Heidelberg New York 1979; Reprint 1997.

[2] N. L. Biggs, E. K. Lloyd & R. J. Wilson: *Graph Theory 1736-1936*, Clarendon Press, Oxford 1976.

[3] A. Cayley: *A theorem on trees*, Quart. J. Pure Appl. Math. 23 (1889), 376-378; Collected Mathematical Papers Vol. 13, Cambridge University Press 1897, 26-28.

[4] A. Joyal: *Une théorie combinatoire des séries formelles*, Advances in Math. 42 (1981), 1-82.

[5] J. Pitman: *Coalescent random forests*, J. Combinatorial Theory, Ser. A 85 (1999), 165-193.

[6] H. Prüfer: *Neuer Beweis eines Satzes über Permutationen*, Archiv der Math. u. Physik (3) 27 (1918), 142-144.

[7] A. Rényi: *Some remarks on the theory of trees*. MTA Mat. Kut. Inst. Kozl. (Publ. math. Inst. Hungar. Acad. Sci.) 4 (1959), 73-83; Selected Papers Vol. 2, Akadémiai Kiadó, Budapest 1976, 363-374.

[8] J. Riordan: *Forests of labeled trees*, J. Combinatorial Theory 5 (1968), 90-103.

填充拉丁方

第 27 章

拉丁方是最古老的组合对象之一, 对它的研究很明显可以追溯到古代. 为得到拉丁方, 人们需要把一个 $(n \times n)$ 方阵的 n^2 个空格用 $1, 2, \cdots, n$ 填上, 使得在每行和每列里面每个数刚好出现一次. 换言之, 行与列各自代表 $\{1, \cdots, n\}$ 的一个排列. 称 n 为这个拉丁方的阶.

1	2	3	4
2	1	4	3
4	3	1	2
3	4	2	1

一个 4 阶拉丁方

我们想要讨论的问题如下: 假设有人开始给方格填充数字 $\{1, 2, \cdots, n\}$. 在某个时刻他停下了, 并让我们把剩下的空格填满以得到拉丁方. 这在什么时候是可能的呢? 当然, 为了有个起码的机会, 我们必须假定: 当我们接手的时候, 每个元素在每行每列至多出现过一次. 给这种情形起个名字: 如果 $(n \times n)$ 方阵的一些空格被 $1, 2, \cdots, n$ 填充, 并且在每行每列中每个数至多出现过一次, 则称之为阶是 n 的*部分拉丁方*. 于是问题即:

1	4	2	5	3
4	2	5	3	1
2	5	3	1	4
5	3	1	4	2
3	1	4	2	5

一个循环拉丁方

在怎样的情形下一个部分拉丁方可以被填满成为同阶的拉丁方?

让我们看几个例子. 假设前 $n-1$ 行都被填上了, 最后一行是空的, 则可轻易填上最后一行. 只须注意每个元素在部分拉丁方里出现了 $n-1$ 次, 所以恰在某一列中不出现. 因此把每个元素写在其缺失的那一列, 我们就正确地填满了方格.

另一个极端, 假设只有第一行被填好了, 仍旧很容易填满方格: 只须在下面的每行逐次循环更迭一位元素.

所以, 尽管在第一个例子里填法是固定的, 第二个例子却有很多种可能. 一般来说, 越少的方格被预先填好了, 我们完成空格有越多的自由.

1	2	$\cdots$	n-1	
				n

一个无法填满的部分拉丁方

尽管如此, 边图所示的部分拉丁方仅被填上了 n 个方格, 但很清楚它不能被完成, 因为没有办法在不违反行或列的规则的情况下填好右上角的方格.

> 如果 $(n\times n)$ 的方阵里只有少于 n 个方格被填好, 那么总能完成剩余的填充得到一个拉丁方吗?

这个问题是 Trevor Evans 在 1960 年提出的; 很快, "填充总是可以的" 这个断言成为 Evans 猜想. 当然, 也许可以试着归纳, 而这正是最后引向成功的方法. 然而 1981 年 Bohdan Smetaniuk 的证明不仅解决了问题, 也是关于归纳证明可以如何精妙地被应用的一个优美范例. 并且这个证明还是构造性的, 它允许我们从某一个初始状态开始可操作地填满拉丁方.

1	3	2
2	1	3
3	2	1

R: 1 1 1 2 2 2 3 3 3
C: 1 2 3 1 2 3 1 2 3
E: 1 3 2 2 1 3 3 2 1

若将上例中的行循环置换, $R\longrightarrow C\longrightarrow E\longrightarrow R$, 则得到下面的线列和拉丁方:

1	2	3
3	1	2
2	3	1

R: 1 3 2 2 1 3 3 2 1
C: 1 1 1 2 2 2 3 3 3
E: 1 2 3 1 2 3 1 2 3

在继续进行证明之前, 让我们看看一般的拉丁方. 换一个角度, 我们可以把拉丁方看作一个 $(3\times n^2)$- 数组, 称为拉丁方的线列. 边图展示了一个 3 阶拉丁方和它的线列, 其中 R, C 和 E 分别表示行、列和元素.

拉丁方上的条件等价于说在线列的任意两行中, 所有的 n^2 个有序对必须出现 (从而每个对出现恰好一次). 显然, 我们可以把每行的元素分别任意置换 (对应于行, 列和元素的重排) 而仍旧得到拉丁方. 但在这个 $(3\times n^2)$- 数组上的条件告诉我们更多: 元素并没有特殊的作用. 我们也可以置换线列的行 (作为整体), 仍旧保持线列的条件, 从而得到的仍是拉丁方.

由任意的这种置换联系在一起的拉丁方称为*共轭*. 下面的观察令证明变得清晰: 一个部分拉丁方显然对应一个部分线列 (任意两行中每个对出现至多一次), 部分拉丁方的共轭仍是部分拉丁方. 特别地, 部分拉丁方可以被补足当且仅当其每个共轭可被补足 (只要补足共轭, 再逆转三行间的置换).

我们将需要两个结果, 它们归功于 Herbert J. Ryser 和 Charles C. Lindner, 比 Smetaniuk 的定理要早. 当一个部分拉丁方的前 r 行被填满了而剩余的方格都是空的, 我们称其为 $(r\times n)$ 的 *拉丁矩*.

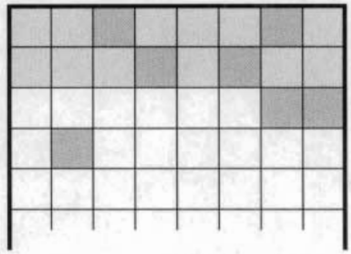
引理 1. *对 $r<n$, 任何 $(r\times n)$ 的拉丁矩都可以扩充为 $((r+1)\times n)$- 拉丁矩, 从而可以补足为拉丁方.*

■ **证明.** 应用 Hall 的定理 (参见第 23 章). 令 A_j 为尚未出现在第 j 列的元素的集合. 规则允许的第 $(r+1)$ 行于是恰好对应 $A_1,\cdots,A_n$ 的一个相异代表系. 因此须验证 Hall 的条件 (H). 每个集合 A_j 的基

数是 $n-r$, 所以每个元素恰在 $n-r$ 个 A_j 里 (因其在矩形中共出现 r 次). 任意 m 个 A_j 包含 $m(n-r)$ 个元素, 于是最少有 m 个不同的, 这正是条件 (H). □

引理 2. 令 P 为一个 n 阶的部分拉丁方, 其中至多填充了 $n-1$ 个方格且所用的不同元素至多有 $\frac{n}{2}$ 个, 则 P 可以被填满成为一个 n 阶拉丁方.

■ **证明.** 先把问题转化为更便捷的形式. 由前面讨论的共轭原理, 可将条件 "至多 $\frac{n}{2}$ 个不同元素" 替换为元素只出现在 $\frac{n}{2}$ 行, 进而还可假设这些行都在最上面. 故设有单位方格被填充的是第 $1, 2, \cdots, r$ 行, 其中第 i 行被填充了 f_i 个单位方格, $r \leqslant \frac{n}{2}$ 且 $\sum_{i=1}^{r} f_i \leqslant n-1$. 通过交换行, 不妨设 $f_1 \geqslant f_2 \geqslant \cdots \geqslant f_r$. 现在一步一步把第 $1, \cdots, r$ 行补满, 直到得到一个 $(r \times n)$- 矩, 然后再根据引理 1 就可以扩充成拉丁方了.



当 $n=8$, $l=3$ 时的情形, $f_1 = f_2 = f_3 = 2$, $f_4 = 1$. 深色方格表示开始已填好的方格, 浅色方格表示在我们的补足过程中填好的.

假设我们已经填满了 $1, 2, \cdots, \ell-1$ 行. 在行 ℓ, 有 f_ℓ 个已填好的方格, 我们可假设都在末端. 现在的情形如图所示, 其中有阴影处表示填好的单元格.

第 ℓ 行的完成是通过另一个 Hall 定理的应用, 但这一次更为精妙. 令 X 为尚未出现在行 ℓ 的元素的集合, 则 $|X| = n - f_\ell$; 而对 $j = 1, \cdots, n-f_\ell$, 令 A_j 表示 X 中尚未出现在第 j 列的元素的集合 (无论在第 ℓ 行的上或下). 所以为补足行 ℓ 我们必须验证族 $A_1, \cdots, A_{n-f_\ell}$ 满足条件 (H).

首先断言

$$n - f_\ell - \ell + 1 > \ell - 1 + f_{\ell+1} + \cdots + f_r. \tag{1}$$

当 $\ell = 1$ 时较为清楚; 否则 $\sum_{i=1}^{r} f_i < n$, $f_1 \geqslant \cdots \geqslant f_r$ 及 $1 < \ell \leqslant r$ 合在一起得到

$$n > \sum_{i=1}^{r} f_i \geqslant (\ell-1) f_{\ell-1} + f_\ell + \cdots + f_r.$$

现在或者 $f_{\ell-1} \geqslant 2$ (此时 (1) 成立) 或者 $f_{\ell-1} = 1$. 后一种情形中 (1) 化为 $n > 2(\ell-1) + r - \ell + 1 = r + \ell - 1$, 由 $\ell \leqslant r \leqslant \frac{n}{2}$ 显然为真.

取 m 个集合 A_j, $1 \leqslant m \leqslant n - f_\ell$, 令 B 为它们的并. 我们证明 $|B| \geqslant m$. 考虑对应 A_j 的这 m 列中含有 X 中元素的方格的个数 c. 至多有 $(\ell-1)m$ 个这样的方格在行 ℓ 之上, 至多 $f_{\ell+1} + \cdots + f_r$

格在行 ℓ 之下, 因此

$$c \leqslant (\ell-1)m + f_{\ell+1} + \cdots + f_r.$$

另一方面, 每个元素 $x \in X \backslash B$ 在这 m 列中都出现, 所以 $c \geqslant m(|X|-|B|)$, 从而 (由 $|X| = n - f_\ell$)

$$|B| \geqslant |X| - \frac{1}{m}c \geqslant n - f_\ell - (\ell-1) - \frac{1}{m}(f_{\ell+1} + \cdots + f_r).$$

这样 $|B| \geqslant m$, 若

$$n - f_\ell - (\ell-1) - \frac{1}{m}(f_{\ell+1} + \cdots + f_r) > m-1,$$

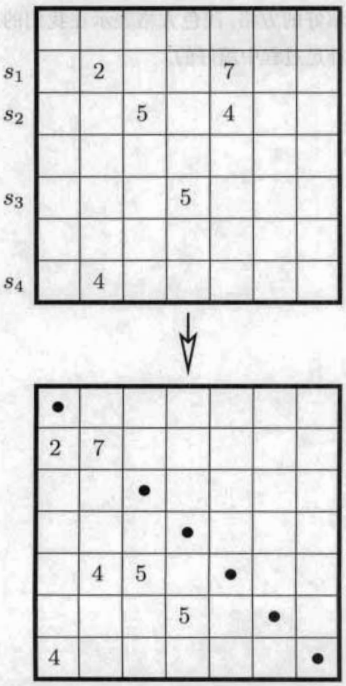
即若

$$m(n - f_\ell - \ell + 2 - m) > f_{\ell+1} + \cdots + f_r. \tag{2}$$

不等式 (2) 当 $m=1$ 时及由 (1) 当 $m = n - f_\ell - \ell + 1$ 时都成立, 所以对所有的 1 和 $n - f_\ell - \ell + 1$ 之间的 m 都成立, 这是因为左端是首项系数为 -1 的 m 的二次函数. 剩下的情形是 $m > n - f_\ell - \ell + 1$. 由于 X 中的每个元素 x 包含在至多 $\ell - 1 + f_{\ell+1} + \cdots + f_r$ 行里面, 其也必出现在不超过这么多的列里面. 再次利用 (1), 我们发现 x 在某个集合 A_j 里, 故此时 $B = X$, $|B| = n - f_\ell \geqslant m$, 证毕. □

最后证明 Smetaniuk 的定理.

定理. *任何一个只填好了至多 $n-1$ 个方格的 n 阶部分拉丁方都可以被填满成为一个同阶的拉丁方.*



■ **证明.** 对 n 归纳, $n \leqslant 2$ 时显然. 现在考虑阶数为 $n \geqslant 3$ 且填好了至多 $n-1$ 个单位方格的部分拉丁方. 沿用前面的符号, 这些小方格在标记为 $s_1, \cdots, s_r$ 的 $r \leqslant n-1$ 个不同的行里, 这些行分别包含 $f_1, \cdots, f_r > 0$ 个填好的小方格, 且 $\sum_{i=1}^{r} f_i \leqslant n-1$. 由引理 2 我们可以假设有多于 $\frac{n}{2}$ 个不同的元素; 由此必有只出现一次的元素: 重新排序及换行 (如果需要的话) 之后不妨设元素 n 仅出现了一次, 而且是在行 s_1 里.

下面我们希望通过置换部分拉丁方的各行各列使得填好的方格都在对角线下方 —— 除了填充的是 n 的那个, 它将在对角线上. (对角线指所有满足 $1 \leqslant k \leqslant n$ 的单位方格 (k,k).) 我们这样来实现: 首先把行 s_1 移到第 f_1 行的位置. 通过对列的置换把所有填好的方格挪到左方, 使得 n 作为这行的最后一个元素出现在对角线上. 接着, 把行 s_2 移到第 $1 + f_1 + f_2$ 行, 仍旧把填好的方格尽量左移. 一般

地, 对 $1 < i \leqslant r$ 把行 s_i 移到第 $1+f_1+f_2+\cdots+f_i$ 行, 再把填好的方格尽量左移. 很明显这给出了想要的结构. 边图是 $n=7$ 时的一个例子: 行 $s_1=2, s_2=3, s_3=5, s_4=7$ 有 $f_1=f_2=2$ 及 $f_3=f_4=1$, 它们分别被移到标号为 2, 5, 6, 7 的行, 列也被 "向左" 置换导致最终除了单独的那个 7 其他的元素都在对角线下方, 对角线则用 • 标识.

为应用归纳法, 现在把 n 从对角线删去, 且忽略第一行及最后一列 (都不含有已经填好的单位格): 这样看到的是填好了至多 $n-2$ 个小方格的 $n-1$ 阶部分拉丁方, 由归纳法可补足为 $n-1$ 阶的拉丁方. 边图显示了前面例子中导出的部分拉丁方的众多补足方法中的一个. 在图中, 原来的小方格被印成深色. 它们已经在最终位置了, 所有阴影中的方格也是; 为完成 n 级的拉丁方, 其他地方的一些方格会在下面的过程中被调换.

2	3	4	1	6	5	
5	6	1	4	2	3	
1	2	3	6	5	4	
6	**4**	**5**	2	3	1	
3	1	6	**5**	4	2	
4	5	2	3	1	6	

下一步, 我们想把对角线上的元素移到最后一列, 再把 n 放进空出的位置. 然而, 一般而言这样不行, 因为对角线上的元素不见得是互异的. 因此我们操作更加谨慎, 对 $k=2,3,\cdots,n-1$ (依此顺序) 逐步进行下面的操作:

把数字 n 放在单位方格 (k,n) 中. 这产生的是正确的部分拉丁方. 现在把对角线上单位方格 (k,k) 中的元素 x_k 和最后一列单位方格 (k,n) 中的元素 n 交换.

若数字 x_k 不是已先存在于最后一列, 则我们在这第 k 步的工作就结束了. 此后, 第 k 列的元素将不需动了.

在我们的例子中当 $k=2,3$ 和 4 时没有问题, 对应的对角线元素 3, 1 , 6 挪到最后一列. 下面三幅图展示了相应的操作.

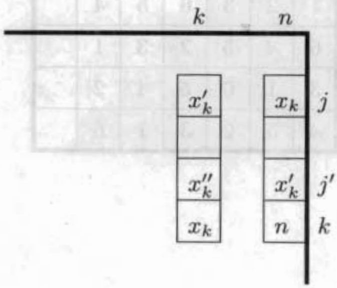
2	3	4	1	6	5	7
5	6	1	4	2	3	
1	2	3	6	5	4	
6	**4**	**5**	2	3	1	
3	1	6	**5**	4	2	
4	5	2	3	1	6	

2	7	4	1	6	5	3
5	6	1	4	2	3	7
1	2	3	6	5	4	
6	**4**	**5**	2	3	1	
3	1	6	**5**	4	2	
4	5	2	3	1	6	

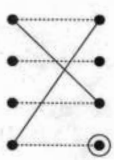
2	7	4	1	6	5	3
5	6	7	4	2	3	1
1	2	3	6	5	4	7
6	**4**	**5**	2	3	1	
3	1	6	**5**	4	2	
4	5	2	3	1	6	

现在我们必须处理当已经有数字 x_k 出现在最后一列时的情形了. 此时我们如下进行:

若已有数字 x_k 在单位方格 (j,n) 中, $2 \leqslant j < k$, 则在行 j 中互换位于第 n 列的元素 x_k 和位于第 k 列的元素 x'_k. 如果 x'_k 也在方格 (j',n) 中, 则我们也在第 j' 行对换第 n 列和第 k 列的元素, 照此继续.



G_k:



如此进行永远不会有两个相同的元素出现在同一行. 我们的交换过程也保证了不会有两个相同元素在同一列. 故只须验证这个交换第 k 列与第 n 列的过程不会导致无穷循环. 这可以从下面的二部图 G_k 看出来: 它的顶点对应那些可能被交换的方格 (i,k) 和 (j,n), $2 \leqslant i,j \leqslant k$. (i,k) 与 (j,n) 之间有边当两者在同一行 (即当 $i=j$), 或者在交换之前两者含有同一个元素 (这意味着 $i \neq j$). 在我们的草图中满足 $i=j$ 的边被画成小圆点拼成的虚线, 其他的则是实线. G_k 的所有顶点的度数是 1 或 2. 小方格 (k,n) 对应一个度数为 1 的顶点; 这个顶点是一条路的一端, 它通过水平线连向第 k 列, 可能又通过一条斜线回到第 n 列, 然后水平地回到第 k 列, 如此下去. 路的另一端是在第 k 列, 其数字不出现在第 n 列. 交换的操作将停止在我们把某个新元素移到最后一列的时候. 然后第 k 列的工作就完成了, 对 $i \geqslant 2$, 方格 (i,k) 将不再动了.

在我们的例子里 "交换情形" 发生在当 $k=5$ 时: 元素 $x_5=3$ 已经在最后一列有了, 所以它必须换到第 $k=5$ 列. 但是这次的交换元 $x'_5=6$ 也不是新的, 故被 $x''_5=5$ 替换, 这次是新的了.

2	7	4	1	6	5	3
5	6	7	4	2	3	1
1	2	3	7	5	4	6
6	4	**5**	2	3	1	7
3	1	6	**5**	4	2	
4	5	2	3	1	6	

2	7	4	1	3	5	6
5	6	7	4	2	3	1
1	2	3	7	6	4	5
6	4	**5**	2	7	1	3
3	1	6	**5**	4	2	
4	5	2	3	1	6	

最终, 当 $k=6=n-1$ 时交换没有问题, 完成后拉丁方就被填满了:

2	7	4	1	3	5	6
5	6	7	4	2	3	1
1	2	3	7	6	4	5
6	**4**	**5**	2	7	1	3
3	1	6	**5**	4	2	7
4	5	2	3	1	6	

2	7	4	1	3	5	6
5	6	7	4	2	3	1
1	2	3	7	6	4	5
6	**4**	**5**	2	7	1	3
3	1	6	**5**	4	7	2
4	5	2	3	1	6	

7	3	1	6	4	2	4
2	7	4	1	3	5	6
5	6	7	4	2	3	1
1	2	3	7	6	4	5
6	**4**	**5**	2	7	1	3
3	1	6	**5**	4	7	2
4	5	2	3	1	6	7

一般地也如此: 把元素 n 放在方格 (n, n) 里, 然后第一行可以被各列缺失的那个元素补足 (见引理 1), 这就结束了证明. 如果想得到补足最初的 n 阶部分拉丁方的明确步骤, 我们只要把证明前两步中的元素, 行和列之间的置换逆回去即可. □

参考文献

[1] T. Evans: *Embedding incomplete Latin squares,* Amer. Math. Monthly **67** (1960), 958-961.

[2] C. C. Lindner: *On completing Latin rectangles,* Canadian Math. Bulletin **13** (1970), 65-68.

[3] H. J. Ryser: *A combinatorial theorem with an application to Latin rectangles,* Proc. Amer. Math. Soc. **2** (1951), 550-552.

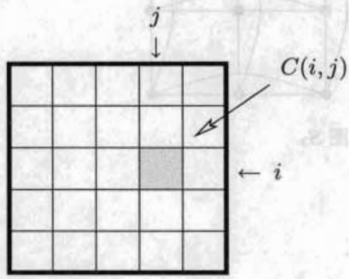
[4] B. Smetaniuk: *A new construction on Latin squares I: A proof of the Evans conjecture,* Ars Combinatoria **11** (1981), 155-172.

Dinitz 问题

第 28 章

四色问题是图论发展到今天的主要推动力之一, 而着色仍旧是很多图论学家最喜欢的一个话题. 下面是 1978 年 Dinitz 提出的一个问题, 听起来简单的一个着色问题却抵挡住了所有的进攻尝试, 直到 15 年后 Fred Galvin 提供了一个简洁到令人震惊的解法.

> 考虑 $(n\times n)$ 方格中的 n^2 个小方格, 令 (i,j) 表示第 i 行和第 j 列处的小方格. 假设对每个小方格 (i,j) 给定某个 n 种颜色的集合 $C(i,j)$.
> 给整个阵列着色, (i,j) 的颜色取自集合 $C(i,j)$, 要求每行每列的颜色两两不同. 这总是可以实现的吗?



开始先考虑所有的颜色集合 $C(i,j)$ 是相同的, 比方说 $\{1,2,\cdots,n\}$ 这一情形. 那么 Dinitz 问题归结到下面的任务: 把 $(n\times n)$- 方阵填上 $1,2,\cdots,n$ 使得每行每列两两不同. 换句话说, 这样的一种着色对应一个拉丁方, 正如前一章里讨论过的. 因此在这种情况下, 问题的答案是肯定的.

既然这里这么容易, 一般地当集合 $C:=\bigcup_{i,j}C(i,j)$ 包含甚至比 n 更多颜色的情形怎么会变得难上那么多呢? 困难在于对一个小方格来说, 并不是 C 里的每种颜色都可以用上. 例如, 尽管在拉丁方里我们显然可以为第一行选择所有颜色的任意置换, 在一般的问题里并非如此. 当 $n=2$ 时这个困难就已显现出来.

$\{1,2\}$	$\{2,3\}$
$\{1,3\}$	$\{2,3\}$

假设我们给定了如图所示的一组颜色集合. 如果我们给第一行选择颜色 1 和 2, 那就有麻烦了: 因为我们将不得不为第二行的两个小方格都选择 3.

在进攻 Dinitz 问题之前, 先用图论的术语复述一下情况. 按惯例考虑无自环无重边的简单图 $G=(V,E)$. 令 $\chi(G)$ 表示该图的色数, 即顶点上最少须用的颜色数使得相邻的顶点必有相异的颜色.

换言之, 着色将 V 划分成等价类 (着成同样颜色的顶点子集) 使得每一类中没有边. 称集合 $A\subseteq V$ 为**独立的**, 如果 A 之内没有边.

从而色数即最小的独立集的个数; 这些独立集应是 V 的一个划分.

1976 年 Vizing 以及三年之后 Erdős, Rubin 和 Taylor, 研究了下面的着色的一种变形, 将我们直接引向 Dinitz 的问题. 设在图 $G = (V, E)$ 中给每个顶点 v 指定了颜色集合 $C(v)$. *列表着色*是一个着色 $c : V \longrightarrow \bigcup_{v \in V} C(v)$ 满足对任意的 $v \in V$ 有 $c(v) \in C(v)$. *列表着色数* $\chi_\ell(G)$ 现在应该清楚了: 即最小的数 k 使得对任意的满足 $|C(v)| = k, \forall v \in V$ 的着色集合 $C(v)$ 的组合, 都存在列表着色. 当然, 有 $\chi_\ell(G) \leqslant |V|$ (颜色不会不够用). 由于普通着色是列表着色当 $C(v)$ 都相同时的特殊情况, 我们知道对任意的图 G

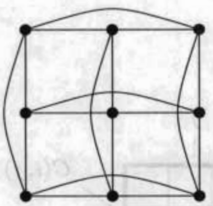


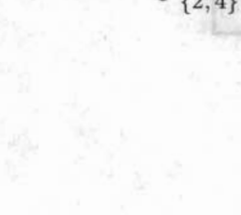
图 S_3

$$\chi(G) \leqslant \chi_\ell(G).$$

为回到 Dinitz 问题, 考虑图 S_n: 其顶点集合为 $(n \times n)$ 阵列的 n^2 个小方格; 两个小方格相邻当且仅当它们在同一行或同一列.

由于一行中的 n 个小方格彼此相邻, 我们需要至少 n 种颜色. 此外, n 种颜色的着色对应拉丁方, 即拉丁方中有同一数字的小方格形成一个颜色类. 如前所见, 拉丁方是存在的, 因此 $\chi(S_n) = n$, Dinitz 问题现在可以简练地叙述为

$$\chi_\ell(S_n) = n?$$



人们或许想 $\chi(G) = \chi_\ell(G)$ 可能对任意的图 G 都对, 但这远非事实. 考察 $G = K_{2,4}$. 因为我们可将左边的两个顶点着上第一种颜色, 右边的顶点用第二种颜色, 其色数为 2. 但现在设想给定了图示的颜色集.

给左边的顶点着色有四种可能 1|3, 1|4, 2|3 和 2|4, 但这里的每一个对都是右边的某个颜色集, 因此列表着色是不可能的. 因此 $\chi_\ell(G) \geqslant 3$, 读者也许会有兴趣去证明 $\chi_\ell(G) = 3$ (并不需要穷举!). 推广这个例子, 不难找到图 G 满足 $\chi(G) = 2$, 而 $\chi_\ell(G)$ 要多大有多大! 所以列表着色问题并不像乍看上去那么简单.

回到 Dinitz 问题. 1992 年 Jeanette Janssen 证明了 $\chi_\ell(S_n) \leqslant n+1$, 这是一个重大突破. 最后一击由 Fred Galvin 完成, 他把两个久为人知的结果创造性地结合在一起. 下面讨论这两个结果, 然后展示它们怎样推出 $\chi_\ell(S_n) = n$.

先固定符号. 对 G 的顶点 v, 如前以 $d(v)$ 表示 v 的度数. 在我们的方格图 S_n 里每个顶点的度数都是 $2n-2$, 由 $n-1$ 个同行的顶点及同样多同列的顶点得来. 对子集 $A \subseteq V$ 用 G_A 表示以 A 为顶

点集且包含 G 中所有在 A 的顶点间的边的子图. 称 G_A 为由 A 导出的子图; 也称 H 为 G 的诱导子图, 若存在某个 A 使得 $H = G_A$.

为陈述第一个结果要用有向图 $\vec{G} = (V, E)$, 即每条边 e 有个走向的图. 符号 $e = (u, v)$ 表示存在起点为 u 终点为 v 的弧 e, 另一种标记方式是 $u \longrightarrow v$. 接下来就可以合理地引入出度 $d^+(v)$ 和入度 $d^-(v)$, 其中 $d^+(v)$ 是以 v 作为起点的边数, 类似的有 $d^-(v)$; 此外, $d^+(v) + d^-(v) = d(v)$. 若书写 G 则意味着 $\vec{G}$ 去掉方向.

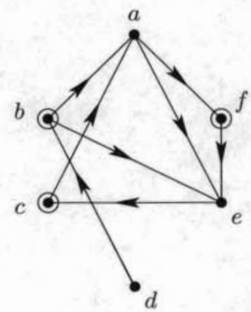
下面的概念来源于游戏分析, 将在我们的讨论中扮演重要角色.

定义 1. 设 $\vec{G} = (V, E)$ 为一个有向图. 它的核 $K \subseteq V$ 是满足如下条件的顶点构成的子集:

(i) K 在 G 中独立.

(ii) 对任意的 $u \notin K$ 存在一个顶点 $v \in K$ 与一条边 $u \longrightarrow v$.

看图中的例子. 子集 $\{b, c, f\}$ 构成了一个核; 另一方面由 $\{a, c, e\}$ 导出的子图没有核, 因为三条边在它的顶点集上循环了一周.



有了这些准备我们可以陈述第一个结果了.

引理 1. *设 $\vec{G} = (V, E)$ 是有向图, 并且对每个顶点 $v \in V$ 有比它的出度大的颜色集 $C(v)$: $|C(v)| \geqslant d^+(v) + 1$. 若 $\vec{G}$ 的每个诱导子图都有核, 则必有 G 的列表着色使得任意 v 的颜色取自 $C(v)$.*

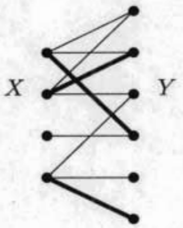
■ **证明.** 对 $|V|$ 归纳. 当 $|V| = 1$ 时无须证明. 选定颜色 $c \in C = \bigcup_{v \in V} C(v)$, 置

$$A(c) := \{v \in V : c \in C(v)\}.$$

由假设, 诱导子图 $G_{A(c)}$ 有核 $K(c)$. 现在将所有的 $v \in K(c)$ 着上颜色 c (这是允许的, 因为 $K(c)$ 是独立集), 再将 $K(c)$ 从 G 中删除, c 从 C 中删除. 令 G' 为 G 在 $V \backslash K(c)$ 上的诱导子图, 且 $C'(v) = C(v) \backslash c$ 是新的颜色集列表. 注意对任意的 $v \in A(c) \backslash K(c)$, 出度 $d^+(v)$ 至少损失了 1 (由核的条件 (ii)). 因此 $d^+(v) + 1 \leqslant |C'(v)|$ 在 $\vec{G}'$ 中仍旧成立. 同样的条件对 $A(c)$ 以外的顶点也成立, 因为在这种情况下颜色集 $C(v)$ 保持不变. 新图 G' 有比 G 更少的顶点, 根据归纳法即得结论. □

进攻 Dinitz 问题的方法现在清楚了: 我们必须找到一个图 S_n 的定向, 对所有的 v 满足出度 $d^+(v) \leqslant n - 1$, 并且对所有的诱导子图保证核的存在性. 这由我们的第二个结果来实现.

我们仍需要一点准备. 回忆 (第 9 章) 二部图 $G = (X \cup Y, E)$ 是具有这样性质的图: 顶点集 V 可分成两部分 X 和 Y 使得每条边有一端在 X 中, 另一端在 Y 中. 换言之, 二部图正是那些可二着色的



二部图和一个匹配

图 (X 用一种颜色, Y 用一种颜色).

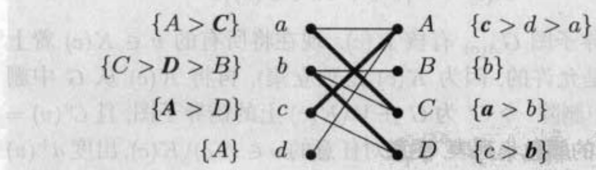
现在介绍一个重要概念 "稳定匹配", 且给一个实际的解释. 二部图 $G=(X\cup Y,E)$ 中的一个*匹配* M 是一组边使得 M 中任两条边没有公共顶点. 图中深色绘出的边构成了一个匹配.

设 X 是某些绅士的集合, Y 是某些女士的集合, $uv\in E$ 意味着 u 和 v 可能会结婚. 匹配从而就是一个杜绝重婚的大规模婚配. 根据我们的目的还需要一个更精细 (也更现实?) 的匹配版本, 这是由 David Gale 和 Lloyd S. Shapley 提出的. 很明显, 现实生活中每个人都有偏好, 而我们把这一点增加到设置上. 在 $G=(X\cup Y,E)$ 中我们假设对每个 $v\in X\cup Y$ 存在其临接点集 $N(v)$ 的一个排序: $N(v)=\{z_1>z_2>\cdots>z_{d(v)}\}$. 于是 z_1 是 v 的 1 号选择, 然后是 z_2, 以此类推.

定义 2. $G=(X\cup Y,E)$ 的匹配 M 称为*稳定的*, 若下面的条件成立: 只要 $uv\in E\backslash M$, $u\in X$, $v\in Y$, 就或者存在 $uy\in M$ 使得在 $N(u)$ 中 $y>v$, 或者存在 $xv\in M$ 使得在 $N(v)$ 中 $x>u$, 或者两者都有.

实际生活中一组婚姻是稳定的, 如果下面的情况永不发生: u 和 v 不是配偶但 u 认为 v 比他的妻子强 (如果他有妻子的话) 而 v 认为 u 比她的丈夫强 (如果她有丈夫的话), 这显然将是不稳定的情况.

在证明第二个结果前看下面的例子:



深色边构成了一个稳定匹配. 在每个优先表上, 引向稳定匹配的那个选择印成黑体.

注意本例中存在唯一的最大匹配 M, 它有 4 条边: $M=\{aC, bB, cD, dA\}$. 但是 M 不稳定 (考虑 cA).

引理 2. *稳定匹配永远存在.*

■ **证明.** 考虑下面的算法. 第一步所有的绅士$u\in X$ 向他们的最爱求婚. 如果一位女士收到了多于 1 个求婚, 就从中选择自己最喜欢的, 把他放进自己的单子; 假如她只收到 1 个求婚, 那当然要保留在单子上. 剩下的男士被拒绝, 集中到保留地 R. 第二步 R 里的男士向他们的第二选择求婚. 女士们比较一下这些求婚 (和自己单子上

的那个, 如果有的话), 选出更偏爱的把他放在单子上. 其他所有人被拒绝形成新的集合 R. 现在 R 里的男士向下一个选择求婚, 如此继续. 如果一位男士向他的最后一个选择求婚仍然被拒, 则将不再被考虑 (也清理出保留地). 显然, 一段时间之后 R 将会清空, 此时算法终止.

断言. *算法终止时, 名单上的男士与对应的女士构成稳定匹配.*

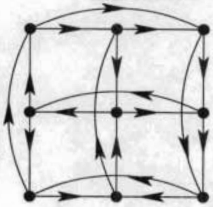
首先注意任何特定的女士单子上的绅士是按照 (那个女士的) 偏好的递增顺序替换上去的, 因为在每一步, 女士拿新的求婚者和当前的绅士作比较, 选择了更喜欢的一个. 所以如果 $uv \in E$ 而 $uv \notin M$, 则或者 u 从来没有向 v 求婚, 亦即他甚至在接触 v 之前就已经找到了更喜欢的人, 意味着 $uy \in M$ 且在 $N(u)$ 中 $y > v$; 或者 u 向 v 求婚但被拒, 表明 $xv \in M$ 且在 $N(v)$ 中 $x > u$. 而这正是稳定匹配的条件. □

综合引理 1 和 2, 我们现在就得到了 Galvin 给 Dinitz 问题的解.

定理. *对任意的 n, 有 $\chi_\ell(S_n) = n$.*

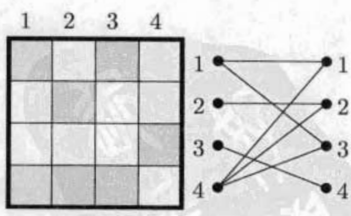
■ **证明.** 如前用 (i,j) 表示 S_n 的顶点, $1 \leqslant i,j \leqslant n$. 于是 (i,j) 与 (r,s) 相邻当且仅当 $i=r$ 或 $j=s$. 取字符集 $\{1,2,\cdots,n\}$ 上的任意拉丁方 L, 用 $L(i,j)$ 表示方格 (i,j) 里面的数字. 接着把 S_n 转换成有向图 $\vec{S}_n$: 当 $L(i,j) < L(i,j')$, 定向为 $(i,j) \longrightarrow (i,j')$; 当 $L(i,j) > L(i',j)$, 定向为 $(i,j) \longrightarrow (i',j)$. 这就是说, 水平地, 我们按照从小的元素往大的元素定向; 竖直地, 正相反. (边图是 $n=3$ 的一个例子.)

1	2	3
3	1	2
2	3	1



注意对所有的 (i,j) 可得 $d^+(i,j) = n-1$. 事实上, 若 $L(i,j)=k$, 则第 i 行的 $n-k$ 个方格里有比 k 大的数字, 而第 j 列的 $k-1$ 个方格里有比 k 小的数字.

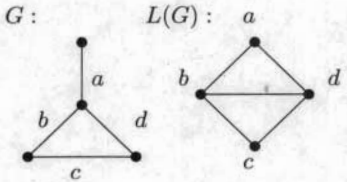
根据引理 1, 剩下的只要证明 $\vec{S}_n$ 的每个诱导子图都有核. 考虑 $A \subseteq V$, 令 X 为 L 的行的集合, Y 为列的集合. 给 A 附加一个二部图 $G=(X \cup Y, A)$, 其中每个 $(i,j) \in A$ 通过边 ij 表示, $i \in X, j \in Y$. 边上的例子中 A 里的小方格加了阴影.



S_n 的定向自然导出 $G=(X \cup Y, A)$ 中邻集的排序: 在 $N(i)$ 中置 $j' > j$, 若在 $\vec{S}_n$ 中有 $(i,j) \longrightarrow (i,j')$; 类似地在 $N(j)$ 中 $i' > i$, 若 $(i,j) \longrightarrow (i',j)$. 由引理 2, $G=(X \cup Y, A)$ 有稳定匹配 M. 这个 M, 看做 A 的一个子集, 正是我们要找的核! 为看到这一点, 首先注意 M 在 A 中是独立的, 因为作为 $G=(X \cup Y, A)$ 中的边它们没有公共的端点 i 或 j. 其次, 若 $(i,j) \in A \backslash M$, 则由稳定匹配的定义存

在或者 $(i,j') \in M$ 使得 $j' > j$, 或者 $(i',j) \in M$ 使得 $i' > i$, 这在 $\vec{S}_n$ 里意味着 $(i,j) \longrightarrow (i,j') \in M$ 或 $(i,j) \longrightarrow (i',j) \in M$. 证毕. □

结束故事以前让我们走得更远一点. 读者也许已经注意到图 S_n 是通过在一个二部图上的简单构造得到的. 取完全二部图, 记为 $K_{n,n}$, $|X| = |Y| = n$, 且边集是 X 与 Y 之间所有的边. 如果我们把 $K_{n,n}$ 所有的边看做某个新图的顶点, 新图中两个顶点相邻当且仅当做为 $K_{n,n}$ 的边它们有一个共同端点, 则清楚地看到这就是方格图 S_n. 让我们把 S_n 称作 $K_{n,n}$ 的线图. 同样的构造可以在任意的图 G 上进行; 称得到的图为 G 的线图 $L(G)$.



线图的构造

一般地, 称 H 为线图若对某个图 G 有 $H = L(G)$. 当然, 并非每个图都是线图. 一个例子是我们先前考虑过的 $K_{2,4}$, 对这个图我们有 $\chi(K_{2,4}) < \chi_\ell(K_{2,4})$. 但如果 H 是线图又怎样呢? 通过修改我们定理的证明易见当 H 是二部图的线图时 $\chi(H) = \chi_\ell(H)$ 成立. 同样的方法也很有可能走得更远来验证这个领域里最后的猜想:

对所有的线图 H 都有 $\chi(H) = \chi_\ell(H)$ 成立吗?

关于这个猜想已知的极少, 看起来很困难 —— 但是毕竟 Dinitz 问题在二十年前也是如此.

参考文献

[1] P. Erdős, A. L. Rubin & H. Taylor: *Choosability in graphs,* Proc. West Coast Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium **26** (1979), 125-157.

[2] D. Gale & L. S. Shapley: *College admissions and the stability of marriage,* Amer. Math. Monthly **69** (1962), 9-15.

[3] F. Galvin: *The list chromatic index of a bipartite multigraph,* J. Combinatorial Theory, Ser. B **63** (1995), 153-158.

[4] J. C. M. Janssen: *The Dinitz problem solved for rectangles,* Bulletin. Amer. Math. Soc. **29** (1993), 243-249.

[5] V. G. Vizing: *Coloring the vertices of a graph in prescribed colours (in Russian),* Metody Diskret. Analiz. **101** (1976), 3-10.

恒等式与双射

第 29 章

考虑无限乘积 $(1+x)(1+x^2)(1+x^3)(1+x^4)\cdots$, 合并乘积中的同类项 x^n, 用通常的方式展成级数 $\sum_{n\geqslant 0} a_n x^n$. 通过观察我们得到前几项

$$\prod_{k\geqslant 1}(1+x^k) = 1+x+x^2+2x^3+2x^4+3x^5+4x^6+5x^7+\cdots. \quad (1)$$

所以我们有比方说 $a_6=4, a_7=5$, 然后可以 (正当地) 猜测当 $n\longrightarrow\infty$ 时, a_n 也趋于无穷.

看同样简单的乘积 $(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots$, 想不到的事情发生了. 展开乘积我们得到

$$\prod_{k\geqslant 1}(1-x^k) = 1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-\cdots. \quad (2)$$

看上去所有的系数等于 1, -1 或 0. 但这是对的吗? 如果是的话, 规律在哪?

无限和与无穷乘积以及它们的收敛性自从微积分诞生以来就在分析领域中扮演核心的角色, 这上面的一些贡献是由数学中的一些最伟大人物做出的, 从 Leonhard Euler 到 Srinivasa Ramanujan.

当解释 (1) 和 (2) 这样的恒等式的时候, 我们却不理会收敛的问题 —— 只是简单地对系数操作, 处理"形式" 幂级数与乘积. 在这个框架下我们将展示组合论证怎样为看似困难的恒等式引出优美证明.

我们的基本概念是自然数的分拆. 我们称满足 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_t\geqslant 1$ 的和式

$$\lambda : n \;=\; \lambda_1+\lambda_2+\cdots+\lambda_t$$

为 n 的一个分拆. $P(n)$ 则是 n 的所有分拆的集合, 且记 $p(n) := |P(n)|$, 其中 $p(0)=1$.

$5=5$
$5=4+1$
$5=3+2$
$5=3+1+1$
$5=2+2+1$
$5=2+1+1+1$
$5=1+1+1+1+1.$

由 $p(5)=7$ 计数的分拆

分拆和我们的问题有什么关系呢? 好, 考虑下面这个无穷多个级数的乘积:

$$(1+x+x^2+x^3+\cdots)(1+x^2+x^4+x^6+\cdots)(1+x^3+x^6+x^9+\cdots)\,\cdots \quad (3)$$

其第 k 项是 $(1+x^k+x^{2k}+x^{3k}+\cdots)$. 当我们把乘积展开成为 $\sum_{n\geqslant 0} a_n x^n$, x^n 的系数是什么呢? 稍加思索就足以说服人们这正是记 n 为和

$$\begin{aligned} n &= n_1\cdot 1+n_2\cdot 2+n_3\cdot 3+\cdots \\ &= \underbrace{1+\cdots+1}_{n_1}+\underbrace{2+\cdots+2}_{n_2}+\underbrace{3+\cdots+3}_{n_3}+\cdots \end{aligned}$$

的方法数. 因此系数就是 n 的分拆数 $p(n)$. 由于几何级数 $1+x^k+x^{2k}+\cdots$ 等于 $\frac{1}{1-x^k}$, 我们证明了第一个恒等式:

$$\prod_{k\geqslant 1}\frac{1}{1-x^k} = \sum_{n\geqslant 0} p(n)\, x^n. \tag{4}$$

进一步, 从以上分析中还可看出因式 $\frac{1}{1-x^k}$ 对应的是 k 对 n 的分拆的贡献. 于是, 假如从 (4) 左端的乘积中忽略 $\frac{1}{1-x^k}$, 那么 k 将不会在右端的任意分拆中出现. 作为例子我们马上就得到

$$\prod_{i\geqslant 1}\frac{1}{1-x^{2i-1}} = \sum_{n\geqslant 0} p_o(n)\, x^n, \tag{5}$$

其中 $p_o(n)$ 是 n 的所有项都是奇数的分拆数. 类似地, 也可得到所有项都是偶数的命题.

$6=5+1$
$6=3+3$
$6=3+1+1+1$
$6=1+1+1+1+1+1$
把 6 分拆为奇数项: $p_o(6)=4$

至此, 无穷积 $\prod_{k\geqslant 1}(1+x^k)$ 中 n 次项的系数是什么应该清楚了. 因为 (3) 中的每个因子或者取 1 或者取 x^k, 这意味着我们考虑的只是每个 k 出现至多一次的分拆. 换句话说, 原来的乘积 (1) 展开为

$$\prod_{k\geqslant 1}(1+x^k) = \sum_{n\geqslant 0} p_d(n)\, x^n, \tag{6}$$

其中 $p_d(n)$ 是 n 的各项互异的分拆数.

$7=7$
$7=5+1+1$
$7=3+3+1$
$7=3+1+1+1+1$
$7=1+1+1+1+1+1+1$

$7=7$
$7=6+1$
$7=5+2$
$7=4+3$
$7=4+2+1.$
7 分别分拆成全奇或互异的部分: $p_o(7)=p_d(7)=5.$

现在形式级数的方法展现了充分的威力. 由 $1-x^2=(1-x)(1+x)$, 可以写

$$\prod_{k\geqslant 1}(1+x^k) = \prod_{k\geqslant 1}\frac{1-x^{2k}}{1-x^k} = \prod_{k\geqslant 1}\frac{1}{1-x^{2k-1}},$$

因为所有偶幂次的因式 $1-x^{2i}$ 都消掉了. 所以, (5) 和 (6) 中的无穷乘积是同一个, 于是级数也相同, 从而得到美妙结果

$$p_o(n) = p_d(n) \qquad 对所有的 n\geqslant 0. \tag{7}$$

如此惊人的等式要求简单的双射证明 —— 至少从任何组合学家的眼光看是这样.

问题. 设 $P_o(n)$ 和 $P_d(n)$ 分别是将 n 分为全是奇数项和全是相异项的分拆: 找到从 $P_o(n)$ 到 $P_d(n)$ 的一个双射!

已知的双射有一些, 但下面这个属于 J. W. L. Glaisher (1907) 的可能是最简洁的. 令 λ 为 n 的一个只有奇数项的分拆. 合并相同的项, 得

$$\begin{aligned} n &= \underbrace{\lambda_1+\cdots+\lambda_1}_{n_1} + \underbrace{\lambda_2+\cdots+\lambda_2}_{n_2} + \cdots + \underbrace{\lambda_t+\cdots+\lambda_t}_{n_t} \\ &= n_1\cdot\lambda_1 + n_2\cdot\lambda_2+\cdots+n_t\cdot\lambda_t. \end{aligned}$$

写出二进制表示 $n_1 = 2^{m_1}+2^{m_2}+\cdots+2^{m_r}$, 类似地处理其他的 n_i. 新的 n 的分拆 λ' 就是

$$\lambda':\ n = 2^{m_1}\lambda_1 + 2^{m_2}\lambda_1+\cdots+2^{m_r}\lambda_1+2^{k_1}\lambda_2+\cdots.$$

我们需要验证 λ' 在 $P_d(n)$ 里面以及 $\phi:\lambda\longmapsto\lambda'$ 确实是双射. 二者都很容易验证: 若 $2^a\lambda_i = 2^b\lambda_j$, 则由 λ_i 和 λ_j 都是奇数有 $2^a=2^b$, 从而 $\lambda_i=\lambda_j$. 因此 λ' 属于 $P_d(n)$. 反之, 若 $n=\mu_1+\mu_2+\cdots+\mu_s$ 是各项互异的分拆, 可通过合并 2 的最高幂次相同的所有 μ_i, 再把奇数写上正确的重数,就逆回去了. 边白展示了一个例子.

例如,

$\lambda: 25 = 5+5+5+3+3+1+1+1+1$

被 ϕ 映到

$$\begin{aligned}\lambda': 25 &= (2+1)5+(2)3+(4)1\\ &= 10+5+6+4\\ &= 10+6+5+4.\end{aligned}$$

写

$\lambda': 30 = 12+6+5+4+3$

为 $30 = 4(3+1)+2(3)+1(5+3)$

$\quad = (1)5+(4+2+1)3+(4)1$

得到分拆 $\phi^{-1}(\lambda')$:

$\lambda: 30 = 5+3+3+3+3+3+3+3+1+1+1+1$

只有奇数项.

于是, 我们运用形式级数引出分拆的等式 $p_o(n)=p_d(n)$, 随后用双射来验证. 现在我们反过来, 先给出分拆的双射证明再推出恒等式. 这次我们的目标是认清展开式 (2) 的规律.

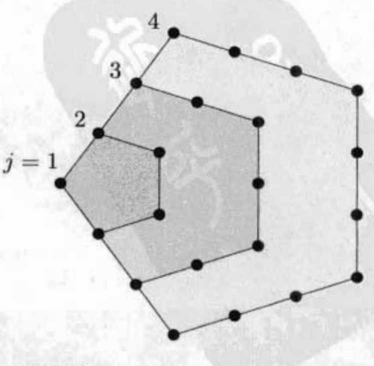
考察

$$1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\cdots.$$

指数 (除了第一个 0) 似乎是成对出现的, 而取每个对里的第一个指数则给出数列

$$1\quad 5\quad 12\quad 22\quad 35\quad 51\quad 70\quad \cdots.$$

众所周知, 这些数与 Euler 有关. 它们就是**五角形数** $f(j)$, 其名字来源参看边图.



五角形数

容易算得 $f(j)=\frac{3j^2-j}{2}$ 以及关于每一对里的另一个有 $\bar f(j)=\frac{3j^2+j}{2}$. 总结一下, 正如 Euler 所做的, 我们猜想下面的公式成立.

定理.

$$\prod_{k\geqslant 1}(1-x^k) \;=\; 1+\sum_{j\geqslant 1}(-1)^j\Big(x^{\frac{3j^2-j}{2}}+x^{\frac{3j^2+j}{2}}\Big). \qquad (8)$$

Euler 通过计算形式级数证明了这一惊人事实, 但我们给出一个双射的天书证明. 首先, 注意到由 (4) 乘积 $\prod_{k\geqslant 1}(1-x^k)$ 恰好是分拆级数 $\sum_{n\geqslant 0}p(n)x^n$ 的逆. 因此, 置 $\prod_{k\geqslant 1}(1-x^k) =: \sum_{n\geqslant 0}c(n)x^n$, 则发现

$$\Big(\sum_{n\geqslant 0}c(n)x^n\Big)\cdot\Big(\sum_{n\geqslant 0}p(n)x^n\Big) \;=\; 1.$$

比较系数, 则$c(n)$ 是唯一的序列满足 $c(0)=1$ 与

$$\sum_{k=0}^{n}c(k)p(n-k) \;=\; 0 \qquad \text{对所有的 } n\geqslant 1. \qquad (9)$$

将 (8) 的右端写作 $\sum\limits_{j=-\infty}^{\infty}(-1)^j x^{\frac{3j^2+j}{2}}$, 我们需要证明

$$c(k) \;=\; \begin{cases} 1 & \text{对}k=\frac{3j^2+j}{2}, \text{当}j\in\mathbb{Z}\text{ 是偶数}, \\ -1 & \text{对}k=\frac{3j^2+j}{2}, \text{当}j\in\mathbb{Z}\text{ 是奇数}, \\ 0 & \text{其他情况}. \end{cases}$$

给出了这个唯一的数列. 对 $j\in\mathbb{Z}$, 置 $b(j)=\frac{3j^2+j}{2}$ 并代入 (9), 我们的猜想简化为

$$\sum_{j\text{ 为偶}}p(n-b(j)) \;=\; \sum_{j\text{ 为奇}}p(n-b(j)) \qquad \text{对所有的 } n.$$

当然我们只须考虑使得 $b(j)\leqslant n$ 的 j. 于是舞台搭好了: 我们必须找到双射

$$\phi:\ \bigcup_{j\text{ 为偶}}P(n-b(j)) \longrightarrow \bigcup_{j\text{ 为奇}}P(n-b(j)).$$

人们提出了好几个双射, 但下面这个由 David Bressoud 和 Doron Zeilberger 给出的构造简单得令人惊讶. 我们只给出 ϕ 的定义 (其事实上是个对合), 请读者自行验证那些简单的细节.

对 $\lambda: \lambda_1 + \cdots + \lambda_t \in P(n - b(j))$, 置

$$\phi(\lambda) := \begin{cases} (t + 3j - 1) + (\lambda_1 - 1) + \cdots + (\lambda_t - 1) & \text{当 } t + 3j \geqslant \lambda_1, \\ (\lambda_2 + 1) + \cdots + (\lambda_t + 1) + \underbrace{1 + \cdots + 1}_{\lambda_1 - t - 3j - 1} & \text{当 } t + 3j < \lambda_1, \end{cases}$$

以上忽略可能存在的那些 0. 可以验证第一种情况下 $\phi(\lambda)$ 在 $P(n - b(j-1))$ 里, 而第二种情况下在 $P(n - b(j+1))$ 里面.

作为例子考虑 $n = 15$, $j = 2$, 于是 $b(2) = 7$. $P(15 - b(2)) = P(8)$ 里的分拆 $3+2+2+1$ 被映射到 $9+2+1+1$, 这是在 $P(15 - b(1)) = P(13)$ 里面.

这真是优美, 而我们还能从中得到更多. 前面已经知道

$$\prod_{k \geqslant 1} (1 + x^k) \;=\; \sum_{n \geqslant 0} p_d(n)\, x^n.$$

有经验的形式级数处理者会引入新的变量 y,然后得到

$$\prod_{k \geqslant 1} (1 + yx^k) \;=\; \sum_{n \geqslant 0} p_{d,m}(n)\, x^n y^m,$$

其中 $p_{d,m}(n)$ 计数 n 的有恰好 m 个互异的项的分拆数. 当 $y = -1$ 时这给出

$$\prod_{k \geqslant 1} (1 - x^k) \;=\; \sum_{n \geqslant 0} (E_d(n) - O_d(n))\, x^n, \qquad (10)$$

其中 $E_d(n)$ 是 n 的全为偶数的互异项的分拆数, 而 $O_d(n)$ 是全为奇数的分拆数. 点睛之笔来了. 比较 (10) 和 (8) 中的 Euler 展开, 我们得到美妙的结果

$$E_d(n) - O_d(n) \;=\; \begin{cases} 1 & \text{对} n = \frac{3j^2 \pm j}{2} \text{ 当} j \geqslant 0 \text{ 为偶数}, \\ -1 & \text{对} n = \frac{3j^2 \pm j}{2} \text{ 当} j \geqslant 1 \text{ 为奇数}, \\ 0 & \text{其他情况}. \end{cases}$$

当 $n = 10$ 时的一个例子:
$10 = 9 + 1$
$10 = 8 + 2$
$10 = 7 + 3$
$10 = 6 + 4$
$10 = 4 + 3 + 2 + 1$
及
$10 = 10$
$10 = 7 + 2 + 1$
$10 = 6 + 3 + 1$
$10 = 5 + 4 + 1$
$10 = 5 + 3 + 2$,
故 $E_d(10) = O_d(10) = 5$.

当然, 这只是一个更长、仍在进行中的故事的开端. 无穷乘积的理论中充满了意料之外的恒等式, 以及它们通过双射对应的对象. 最著名的例子是所谓的 Rogers-Ramanujan 恒等式, 它根据 Leonard Rogers 和 Srinivasa Ramanujan 命名, 在其中数字 5 起了神秘作用:

$$\prod_{k \geqslant 1} \frac{1}{(1 - x^{5k-4})(1 - x^{5k-1})} \;=\; \sum_{n \geqslant 0} \frac{x^{n^2}}{(1-x)(1-x^2)\cdots(1-x^n)},$$

$$\prod_{k \geqslant 1} \frac{1}{(1 - x^{5k-3})(1 - x^{5k-2})} \;=\; \sum_{n \geqslant 0} \frac{x^{n^2+n}}{(1-x)(1-x^2)\cdots(1-x^n)}.$$



Srinivasa Ramanujan

我们邀请读者来将它们表达成下面的分拆恒等式, 这是由 Percy MacMahon 首先注意到的:

- 令 $f(n)$ 为 n 的所有项都形如 $5k+1$ 或 $5k+4$ 的分拆数, $g(n)$ 为任意两项相差至少为 2 的分拆数, 则 $f(n)=g(n)$.
- 令 $r(n)$ 为 n 的所有项都形如 $5k+2$ 或 $5k+3$ 的分拆数, $s(n)$ 为任意两项相差至少为 2 并且不含项 1 的分拆数, 则 $r(n)=s(n)$.

所有已知的 Rogers-Ramanujan 恒等式的形式级数证明都相当复杂. 在很长的时期内, $f(n)=g(n)$ 和 $r(n)=s(n)$ 的双射证明似乎无迹可寻; 这样的证明终于在 1981 年由 Adriano Garsia 和 Stephen Milne 给出. 然而, 它们的双射非常复杂 —— 天书证明还看不到踪影.

参考文献

[1] G. E. Andrews: *The Theory of Partitions,* Encyclopedia of Mathematics and its Applications, Vol. 2, Addison-Wesley, Reading MA 1976.

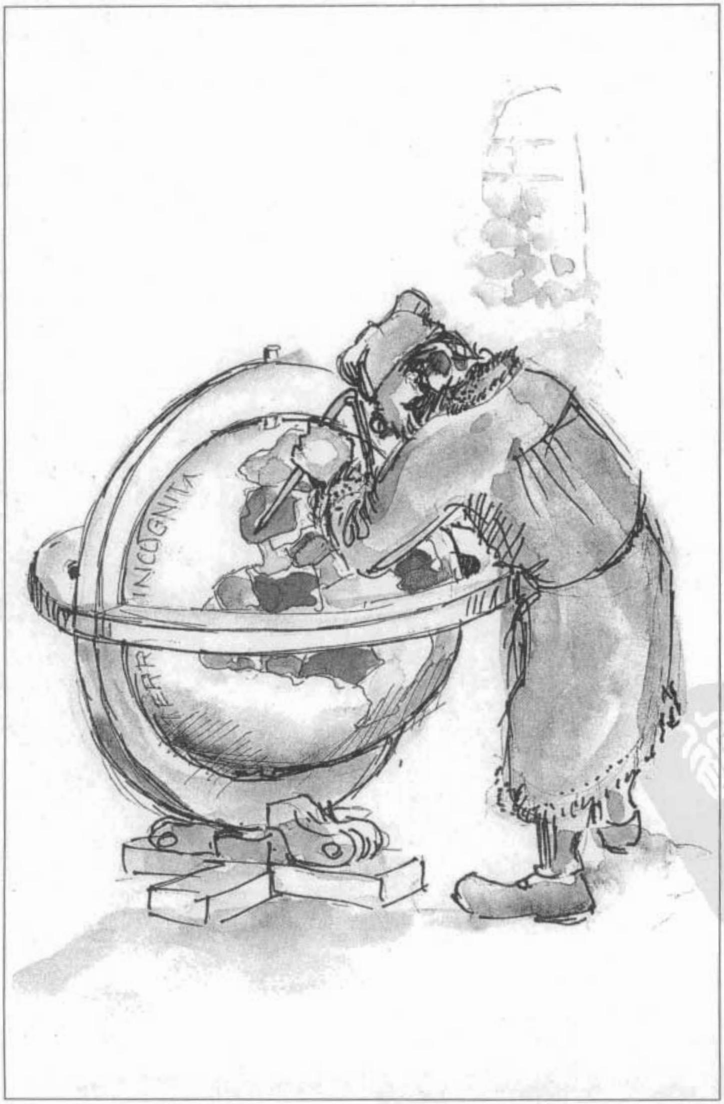
[2] D. Bressoud & D. Zeilberger: *Bijecting Euler's partitions-recurrence,* Amer. Math. Monthly **92** (1985), 54-55.

[3] A. Garsia & S. Milne: *A Rogers-Ramanujan bijection,* J. Combinatorial Theory, Ser. A **31** (1981), 289-339.

[4] S. Ramanujan: *Proof of certain identities in combinatory analysis,* Proc. Cambridge Phil. Soc. **19** (1919), 214-216.

[5] L. J. Rogers: *Second memoir on the expansion of certain infinite products,* Proc. London Math. Soc. **25** (1894), 318-343.

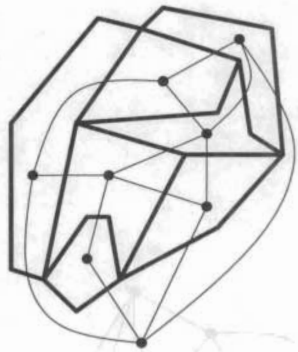
图 论



四色地图

第 30 章 平面图的五色问题

在图论建立之初, 平面图以及它们的着色问题就成为研究的热点, 这是因为它们和四色问题有着密切的联系. 最初的四色问题是: 是否总可以用四种颜色着色平面图的区域, 使得图中共边的区域 (不仅仅是一个点) 有不同的颜色. 右图表明着色图的区域等价于着色平面图的顶点. 如第 11 章所讲, 将一顶点放入每个区域的内部 (包含外面的区域), 然后将相邻区域中的两个顶点连接起来, 且连线要通过公共边.



图的对偶图

这样生成的图 G 是 M 的对偶图, 它是一个平面图, 且一般意义下着色 G 的顶点相当于着色 M 的区域. 因此我们只需研究顶点的着色问题. 我们可以假设图 G 没有自环和重边, 因为这两个概念与着色无关.

在漫长且艰辛尝试证明四色问题的历史中, 有许多非常接近的结果, 但是最终成功的是 Appel-Haken 在 1976 年的证明和 Robertson, Sanders, Seymour 和 Thomas 在 1997 年运用古老组合思想的证明 (可以追溯到 19 世纪) 以及最新的用现代计算机的证明. 原始证明问世 25 年以来, 并没有得到明显的改进.

因此让我们退一步想, 是否存在一个简洁的证明可以说明任何平面图可以五着色. 在上个世纪初, Heawood 给出了这个定理的证明. 他的证明中运用到的基本工具 (事实上在四色定理中也用到了) 是 Euler 公式 (见第 11 章) . 显然, 当给 G 着色时, 我们可以假设 G 是连通的, 因为我们可以分别着色连通块. 一个平面图将平面分成 R 个区域 (包含最外面的区域) . Euler 公式表明对于任何连通平面图 $G = (V, E)$, 我们有



这个平面图有 8 个顶点, 13 条边以及 7 个区域.

$$|V| - |E| + |R| = 2.$$

作为一个热身, 我们先看看如何运用 Euler 公式去证明每个图都可以六着色. 我们对顶点数 n 进行归纳. 对于比较小的 n (特别地对于 $n \leqslant 6$) 这是很显然的.

从第 11 章命题的 (A) 部分 我们知道 G 有一个度数至多为 5 的

顶点 v. 删去 v 以及和它相连的所有边, 则得到顶点数为 $n-1$ 的平面图 $G' = G\backslash v$, 根据归纳法, 它可以被六着色. 因为 v在 G 中至多有 5 个邻点, 所以在图 G' 中至多用五种颜色来着色这些邻点. 如果我们可以用在图 G' 中没有用来着色 v 的邻点的颜色来着色 v, 这样我们将 G' 的六色方案扩充成 G 的六色方案.

现在让我们来看看平面图的列表色数, 我们已经在 Dinitz 问题那章讨论过这个问题了. 显然地, 六色问题的方法也可以用到列表色数上 (同样, 我们不会用完颜色), 因此对每个平面图 G 有 $\chi_\ell(G) \leqslant 6$ 成立. 1979 年, Erdős, Rubin 和 Taylor 猜想所有的平面图的列表色数最多是 5, 且存在列表色数满足 $\chi_\ell(G) > 4$ 的平面图 G. 他们的猜想都是对的. Margit Voigt 第一次构造了一个列表色数为 $\chi_\ell(G) = 5$ 的平面图 G (她所举的例子含有 238 个顶点), 且几乎在同一样时间 Carsten Thomassen 给出了一个关于五列表着色猜想的绝妙证明. 他的证明也生动地告诉了我们: 当你发现正确的归纳假设之后你就知道该怎么做了. 他的这个证明没有运用到 Euler 公式!



近似三角剖分平面图

定理. *所有平面图 G 可以五列表着色, 即:*

$$\chi_\ell(G) \leqslant 5.$$

■ **证明.** 首先注意到增加边只会增加图的色数. 换言之, 如果 H 是 G 的子图, 则有$\chi_\ell(H) \leqslant \chi_\ell(G)$. 因此我们可以假设 G 是连通的且所有嵌入平面的边界都是三角形. 我们称这样的图为*近似三角剖分平面图*. 由这个定理关于近似三角剖分平面图的证明可以建立这个定理关于所有平面图的证明.

证明这个定理的窍门就是证明以下非常强的陈述 (我们将用归纳法证明):

令 $G=(V,E)$ 是一个近似三角剖分图, B 是最外面区域的边界. 我们在颜色集 $C(v)$, $v \in V$ 上作如下假设:

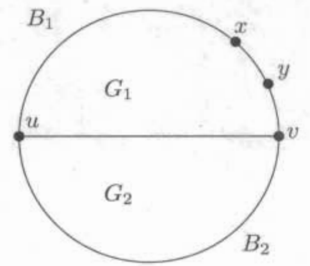
(1) B 中两个相邻的顶点 x, y 已经着上了不同的颜色 α 和 β.

(2) 对于任意 B 中的顶点 v 有 $|C(v)| \geqslant 3$.

(3) 对于任意内顶点 v 有 $|C(v)| \geqslant 5$.

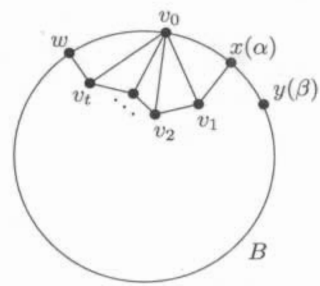
则通过从颜色列表中选择颜色, 可以将 x, y 的着色扩充成 G 的一个正常着色, 特别地, $\chi_\ell(G) \leqslant 5$.

对于 $|V| = 3$ 这是显然的, 因为对于唯一没有着色的顶点 v 我们有 $|C(v)| \geqslant 3$, 因此存在可用的颜色. 现在我们采用归纳法.



情形 1. 设 B 有一条连接两顶点 $u, v \in B$ 的弦, 它并不在 B 中. 由归纳假设, 被 $B_1 \cup \{uv\}$ 包围且包含顶点 x, y, u 和 v 的子图 G_1 是近似三角剖分的, 因此是可以被五着色的. 设在这个着色方案中顶点 u 和 v 得到的颜色是 γ 和 δ. 现在让我们看看被 B_2 和 uv 包围的底下部分 G_2. 考虑到 u, v 是被先着色的, 则我们知道 G_2 也满足归纳假设. 因此 G_2 存在五列表着色, 故 G 也是.

情形 2. 假设 B 没有弦. 设 v_0 是位于 B 上被着成 α 色的顶点 x 的另一侧的顶点, $x, v_1, \cdots, v_t, w$ 是 v_0 的邻点. 因为 G 是近似三角剖分的, 故我们得到如图所示的情形.



通过从 G 删去顶点 v_0 以及所有与其相连的边, 我们构造了近似三角剖分图 $G' = G \backslash v_0$. G' 有外边界 $B' = (B \backslash v_0) \cup \{v_1, \cdots, v_t\}$. 根据假设 (2)有$|C(v_0)| \geqslant 3$, 我们知道 $C(v_0)$ 中存在两个不同于 α 的颜色 γ 和 δ. 现在我们用 $C(v_i) \backslash \{\gamma, \delta\}$ 去替代每个 $C(v_i)$, 并且保持 G' 中其他顶点的着色方案. 则 G' 显然满足所有假设且根据归纳假设它存在五列表着色. 为 v_0 着上不同于颜色 w 的颜色 γ 或者 δ, 这样我们就可以把 G' 的列表着色扩充到整个 G 上. □

这样我们就证明了五列表着色定理. 但是, 故事并没有完. 一个更强的猜测声称: 一个平面图 G 的列表着色的色数最多比其一般着色的色数多 1.

对于任意平面图 G 是否有 $\chi_\ell(G) \leqslant \chi(G) + 1$?

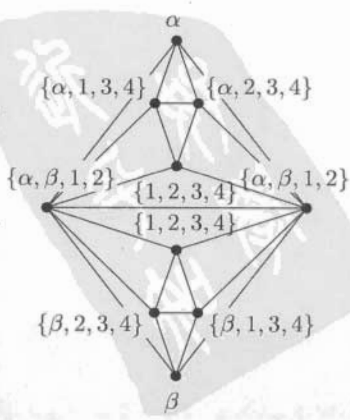
因为根据四色定理 $\chi(G) \leqslant 4$, 我们得到以下三种情形:

情形 I: $\chi(G) = 2 \implies \chi_\ell(G) \leqslant 3$

情形 II: $\chi(G) = 3 \implies \chi_\ell(G) \leqslant 4$

情形 III: $\chi(G) = 4 \implies \chi_\ell(G) \leqslant 5$.

Thomassen 的结果解决了情形 III, Alon 和 Tarsi 巧妙地 (且非常复杂) 证明了情形 I. 更进一步, 存在 $\chi(G) = 2$ 和 $\chi_\ell(G) = 3$ 的图 G, 例如在前面关于 Dinitz 的问题的那一章所提到的图 $K_{2,4}$.



关于情形 II 呢? 这个猜测是不对的: 基于早期由 Shai Gutner 构造的一个图, Margit Voigt 第一次证明了这个结论. Shai Gutner 用如下方法构造了这个具有 130 个顶点的图. 首先让我们看看如图所示的"双八面体", 它显然可以被三着色. 令$\alpha \in \{5, 6, 7, 8\}$, $\beta \in \{9, 10, 11, 12\}$, 且考虑如图所示的列表. 你可以证明用这些列表去着色该图是不可能的: 现在我们将这个图复制 16 倍, 把所有顶部的

顶点和底部的顶点看成一样的. 这样我们得到 $16 \cdot 8 + 2 = 130$ 个顶点的平面图, 它仍是三着色图. 我们把 $\{5,6,7,8\}$ 分配给顶部的顶点, $\{9,10,11,12\}$ 分配给底部的顶点, 16 对 (α,β) ($\alpha \in \{5,6,7,8\}$, $\beta \in \{9,10,11,12\}$) 分配给内部的顶点. 对于 α 和 β 的每个选择, 我们得到如图的一个子图, 而且整个大图的列表着色是不可能的.

通过修改 Gutner 的另一个例子, Voigt 和 Wirth 得到一个更小的图, 它有 75 个顶点, $\chi = 3$, $\chi_\ell = 5$, 而且其最小列表着色是 5. 现在的纪录是 63 个顶点.

参考文献

[1] N. Alon & M. Tarsi: *Colorings and orientations of graphs,* Combinatorica **12** (1992), 125-134.

[2] P. Erdős, A. L. Rubin & H. Taylor: *Choosability in graphs,* Proc. West Coast Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium **26** (1979), 125-157.

[3] S. Gutner: *The complexity of planar graph choosability,* Discrete Math. **159** (1996), 119-130.

[4] N. Robertson, D. P. Sanders, P. Seymour & R. Thomas: *The four-colour theorem,* J. Combinatorial Theory, Ser. B **70** (1997), 2-44.

[5] C. Thomassen: *Every planar graph is* 5*-choosable,* J. Combinatorial Theory, Ser. B **62** (1994), 180-181.

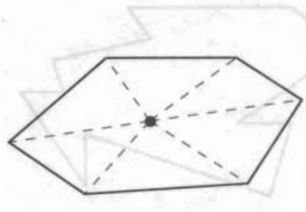
[6] M. Voigt: *List colorings of planar graphs,* Discrete Math. **120** (1993), 215-219.

[7] M. Voigt & B. Wirth: *On* 3*-colorable non-*4*-choosable planar graphs,* J. Graph Theory **24** (1997), 233-235.

博物馆的保安

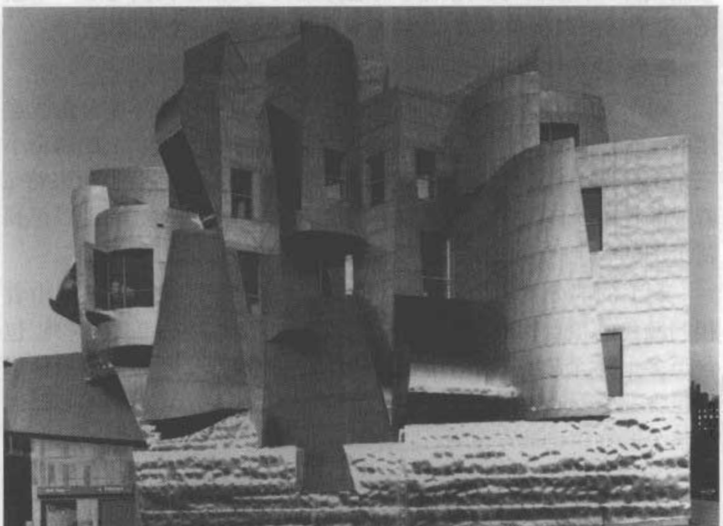
第 31 章

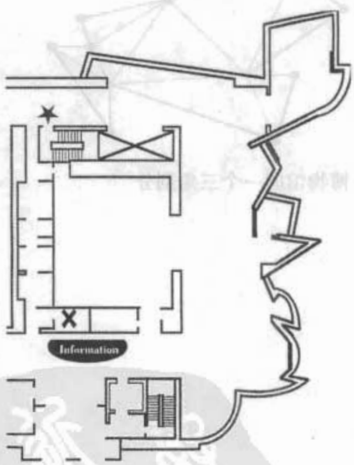
1973 年, Victor Klee 提出了一个非常吸引人的问题. 假设一个博物馆的经理想确保任何时刻博物馆的每个地方都可被一名保安观察到. 如果保安在固定的位置上, 且他们可以转动, 那么这个博物馆总共需要多少保安呢?



一个凸的展览馆

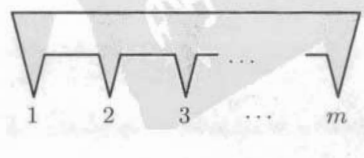
我们将博物馆的墙画成具有 n 个顶点的多边形. 当然, 如果这个多边形是凸的, 那么一个保安就够了. 事实上, 保安驻扎在任何一个位置都可以. 但是一般情况下, 展览馆的墙可以是任何形状的闭多边形.



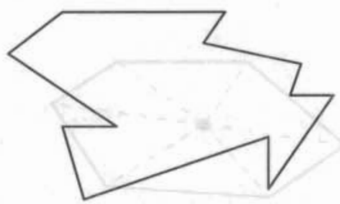


一个现实生活中的美术馆 $\cdots$

如边图所示, 考虑一个墙数为 $n = 3m$ 梳子形博物馆. 易见, 这个博物馆至少需要 $m = \frac{n}{3}$ 个保安. 事实上, 这有 n 面墙. 现在点 1 只能被安置在包含 1 的阴影三角形内的保安观察到, 对于其他点 $2, 3, \cdots, m$ 有类似的情况. 因为所有三角形都是不相交的, 故我们得到结论: 这个博物馆至少需要 m 个保安. 但是 m 个保安足够



了, 因为他们被安排在三角形的顶部的边上. 去掉最后的一或两面墙, 我们得到对于任意 n 存在一个需要 $\lfloor \frac{n}{3} \rfloor$ 个保安的 n 面墙博物馆.

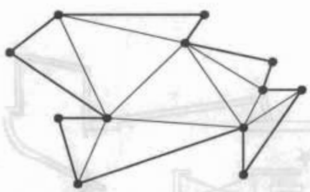


具有 $n = 12$ 面墙的博物馆

以下的结果陈述了这是最坏的情况.

定理. 对于任意一个有 n 面墙的博物馆, $\lfloor \frac{n}{3} \rfloor$ 个保安就足够了.

这个"美术馆定理"首先是被 Vašek Chvátal 用一个非常聪明的论证证明的, 但是这里给出的 Steve Fisk 的证明实在是漂亮.



博物馆的一个三角剖分

■ **证明.** 首先, 让我们在拐角处画 $n-3$ 条不交叉的对角线直到博物馆被三角剖分. 例如, 我们可以在图中画 9 条对角线来产生一个三角剖分. 本证明与三角剖分的选择无关. 现在让我们考虑一个新图: 这个新图以拐角为顶点, 墙和对角线为边的一个平面图.

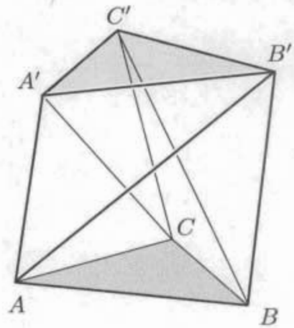
断言. 这个图可以三着色.

对于 $n = 3$, 这个结论是显然的. 现在对 $n > 3$ 选择被对角线连接的两个顶点 u 和 v. 这个对角线可以将图分成包含边 uv 的两个小三角剖分图. 根据归纳假设, 我们将每部分三着色, 且我们可以将 u 着成颜色 1, v 着成颜色 2. 将这两个着色方案联合起来, 就可以得到整个图的一个三着色方案.

剩下的部分就比较简单了. 因为有 n 个顶点, 至少有一族由着相同颜色的顶点构成的顶点类, 比如说被着成颜色 1 的顶点类, 包含至多 $\lfloor \frac{n}{3} \rfloor$ 个顶点, 我们就在这些地方安排保安. 因为每个三角形都包含一个着成颜色 1 的顶点, 我们知道每个三角形都被守卫着, 因此整个博物馆也被守卫着. □

聪明的读者也许会发现我们论证过程中有一个微妙的地方: 是否总是存在这样一个三角剖分呢? 大概每个人的第一反应都是: 显然存在啊! 是的, 这是存在的, 但是完全不是显而易见的, 且事实上, 这个事实不能推广到三维情形 (分成两个四面体)! 这个可以从边图所示的 *Schönhardt* 多面体看出来. 边图是将一个三角棱柱绕顶部三角形旋转而得到的, 但是每个四边形的面被分成拥有非凸边的两个三角形. 试着三角剖分这个多面体! 你会发现任何包含底部三角形的四面体一定包含顶部的三个顶点中的一个: 但是所得到的四面体

不会被包含在 Schönhardt 多面体中. 因此, 如果没有附加的顶点, 就不存在三角剖分.

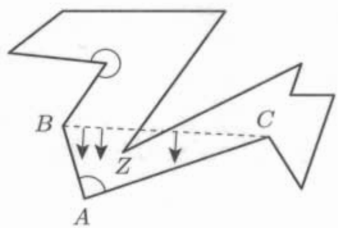


Schönhardt 多面体: 边 AB', BC' 和 CA' 的内部二面角大于 180°.

为了证明平面非凸多边形存在一个三角剖分, 我们对顶点数 n 进行归纳. 对于 $n = 3$ 的情形是显而易见的. 令 $n \geqslant 4$, 根据归纳法, 我们只需要找到将多边形 P 分成两部分的一条对角线, 使得多边形的三角剖分是由其部分的三角剖分粘合而成.

如果顶点 A 的内角是小于 180° 的, 则称顶点 A 是凸的. 因为 P 的所有内角之和是 $(n-2)180°$, 所以 P 存在一个凸顶点 A. 事实上, 至少存在三个凸顶点: 本质上这是鸽笼原理的一个应用! 或者你可以考虑多边形的凸包, 且注意到它的所有凸顶点对于原始多边形也是凸的.

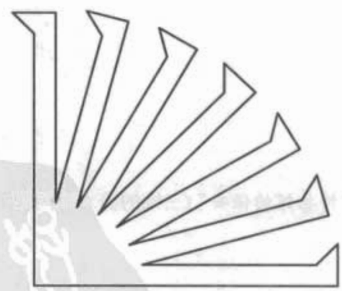
现在我们考虑 A 的两个相邻顶点 B 和 C. 如果线段 BC 都在 P 里, 则这就是我们的对角线. 如果不是, 则三角形 ABC 包含其他顶点. 将 BC 滑向 A 直到它碰上 ABC 中的最后一个顶点 Z. 现在 AZ 是在 P 里, 所以我们得到一条对角线.



现在存在许多关于美术馆定理的不同变形. 例如, 我们可能只须守卫墙壁 (因为, 那是挂画的地方) , 或者保安都被安置在顶点上. 如下是一个特别好的 (未解决) 的变形:

> 假设每个保安只需巡逻博物馆的一面墙, 因此他沿着这面墙走并且可以看到从墙上任何一点能够看到的任何事情.
> 我们需要多少个这样的"墙保安"来维持秩序呢?

Godfried Toussaint 构造了一个如图所示博物馆, 这个博物馆需要 $\lfloor \frac{n}{4} \rfloor$ 个墙保安.



这个多边形有 28 条边 (一般地设为 $4m$ 条边) , 请读者证明这样的情形需要 m 个墙保安. 有猜测说除了一些很小的值 n, 这个数也是足够的, 但这个猜测还没有得到证实.

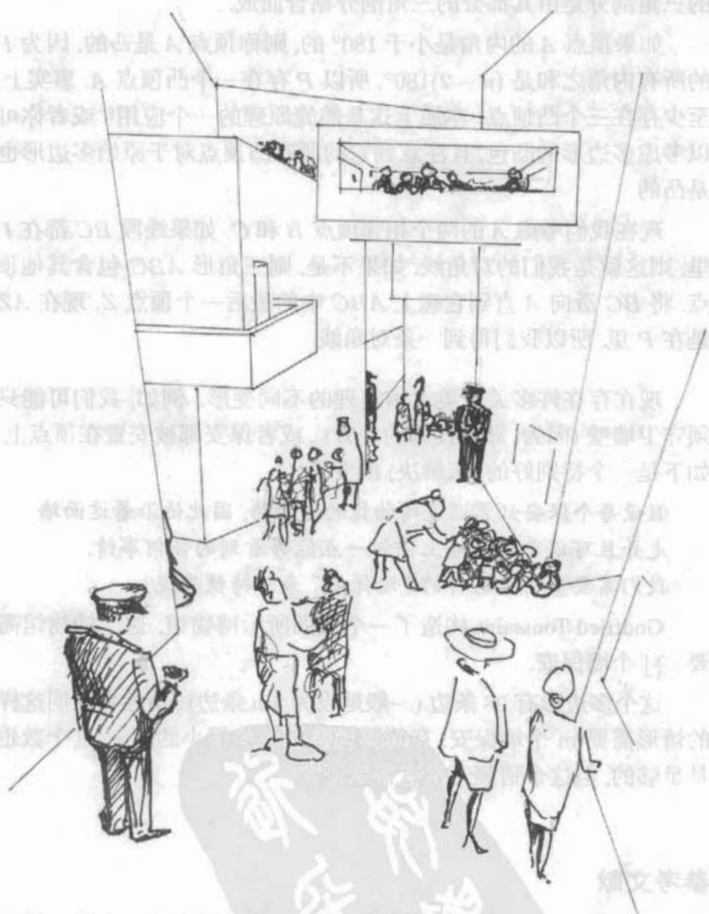
参考文献

[1] V. Chvátal: *A combinatorial theorem in plane geometry,* J. Combinatorial Theory, Ser. B **18** (1975), 39-41.

[2] S. Fisk: *A short proof of Chvátal's watchman theorem,* J. Combinatorial Theory, Ser. B **24** (1978), 374.

[3] J. O'Rourke: *Art Gallery Theorems and Algorithms,* Oxford University Press 1987.

[4] E. Schönhardt: *Über die Zerlegung von Dreieckspolyedern in Tetraeder,* Math. Annalen **98** (1928), 309-312.



"博物馆的保安"(三维的美术馆问题)

Turán 的图定理

第 32 章

图论中最基本的定理之一是 1941 由 Turán 发现的一个定理, 它开启了极图理论的研究. Turán 的定理被多次重新发现有许多证明方法. 本章中, 我们将讨论其中的五个, 请读者判断哪个证明属于数学天书.

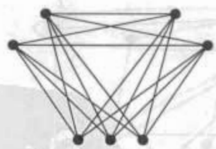


Paul Turán

让我们先固定一些符号. 我们考虑顶点集 $V = \{v_1, \cdots, v_n\}$ 和边集 E 上的简单图 G. 如果 $v_iv_j \in E$ 则称 v_i 和 v_j 是相邻的. 如果 G 中的一个 p- 团是 p 个顶点的完全子图, 则标记它为 K_p. Paul Turán 提出了以下问题:

> 设 G 是一个简单图且不包含 p- 团, 则 G 最多有几条边?

我们把 V 分成 $p-1$ 对互不相交的子集 $V = V_1 \cup \cdots \cup V_{p-1}$, $|V_i| = n_i, n = n_1 + \cdots + n_{p-1}$ 并将从属于不同的 V_i, V_j 中的顶点连接起来, 从而得到这样的子图的例子. 我们记得到的图为 $K_{n_1,\cdots,n_{p-1}}$, 它有 $\sum_{i<j} n_in_j$ 条边. 给定 n, 如果我们尽可能地将 n 分成差不多大小的 n_i, 即对于任意 i, j 有 $|n_i - n_j| \leqslant 1$, 我们将得到这类图中最大的边数. 事实上, 假设 $n_1 \geqslant n_2 + 2$. 将 V_1 中的一个顶点放到 V_2 中, 我们得到边数比图 $K_{n_1,n_2,\cdots,n_{p-1}}$ 多 $(n_1-1)(n_2+1) - n_1n_2 = n_1 - n_2 - 1 \geqslant 1$ 的图 $K_{n_1-1,n_2+1,\cdots,n_{p-1}}$. 我们称满足 $|n_i - n_j| \leqslant 1$ 的图 $K_{n_1,\cdots,n_{p-1}}$ 为*Turán* 图. 特别地, 如果 n 被分成 $p-1$ 份, 则我们可以对所有的 i 令 $n_i = \frac{n}{p-1}$, 从而得到



图$K_{2,2,3}$

$$\binom{p-1}{2}\left(\frac{n}{p-1}\right)^2 = \left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}$$

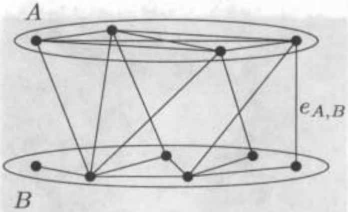
条边. Turán 的定理表明这个数是任意无 p- 团的 n 顶点图的边数的一个上界.

定理. 如果具有 n 个顶点的图 $G = (V, E)$ 没有 p- 团且 $p \geqslant 2$, 则

$$|E| \leqslant \left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}. \tag{1}$$

当 $p=2$ 时这是显而易见的. 我们感兴趣的第一个数是 $p=3$, 在这种情况下, 定理表明不含三角形的 n 顶点图的边数最多是 $\frac{n^2}{4}$. 在 Turán 的结果之前, 这个特殊情况已经被证明. 第 17 章讲了两个运用不等式的漂亮证明.

现在我们来看看一般情形. 首先, 我们介绍分别由 Turán 和 Erdős 给出的基于归纳法的两个证明.

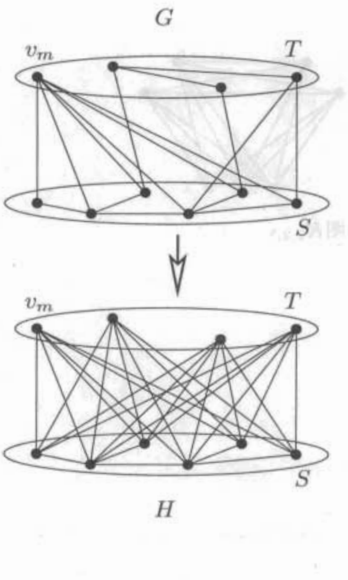


■ **第一个证明.** 我们对 n 进行归纳. 很容易验证当 $n<p$ 时, (1) 成立. 令 G 为点集 $V=\{v_1,\cdots,v_n\}$ 上包含最多边的无 p- 团图且 $n\geqslant p$. G 一定包含 $(p-1)$- 团, 否则我们可以加入一些边. 设 A 是一个 $(p-1)$- 团, 且令集合 $B:=V\backslash A$.

A 包含 $\binom{p-1}{2}$ 条边, 且现在我们估计 B 中的边数 e_B 以及 A 和 B 之间的边数 $e_{A,B}$. 根据归纳法, 我们有 $e_B\leqslant\frac{1}{2}(1-\frac{1}{p-1})(n-p+1)^2$. 因为 G 没有 p- 团, 每个 $v_j\in B$ 最多与 A 中 $p-2$ 个顶点相连, 我们有 $e_{A,B}\leqslant(p-2)(n-p+1)$. 综合起来, 我们得到

$$|E|\leqslant\binom{p-1}{2}+\frac{1}{2}\Big(1-\frac{1}{p-1}\Big)(n-p+1)^2+(p-2)(n-p+1),$$

右边恰好是 $(1-\frac{1}{p-1})\frac{n^2}{2}$. □



■ **第二个证明.** 这个证明充分利用了 Turán 图的结构. 令 $v_m\in V$ 是度数最大的顶点, 即 $d_m=\max_{1\leqslant j\leqslant n}d_j$. 用 S 表示由 v_m 的邻点构成的集合, $|S|=d_m$, 且令 $T:=V\backslash S$. 由于 G 中没有 p- 团, 且 v_m 是与 S 中的所有点相邻的, 我们知道 S 中没有 $(p-1)$- 团.

现在我们在 V 上构造图 H (如图所示) . H 对应着 S 上的 G 且包括 S 与 T 之间的所有边, 但不包含 T 中的边. 换言之, T 是 H 中的独立集, 我们得到结论: H 中也没有 p- 团. 设 d'_j 是 H 中顶点 v_j 的度数. 如果 $v_j\in S$, 则我们根据 H 的构造可以知道 $d'_j\geqq d_j$, 且对于 $v_j\in T$, 通过 v_m 的选择我们有 $d'_j=|S|=d_m\geqslant d_j$. 我们推断出 $|E(H)|\geqslant|E|$, 且在所有具有最大边数的图中一定存在具有 H 形式的图. 根据归纳法, 由 S 诱导的图至多和 S 上的一个合适的 $K_{n_1,\cdots,n_{p-2}}$ 图具有相同的边数. 因此由 $|E|\leqslant|E(H)|\leqslant E(K_{n_1,\cdots,n_{p-1}})$ 和 $n_{p-1}=|T|$, 我们推断出 (1). □

接下来的两个证明与上述证明具有不同的性质, 它们运用了最大值论证和概率论中的思想. Motzkin 和 Straus 以及 Alon 和 Spencer 分别得到了这个证明.

■ **第三个证明.** 考虑顶点上的概率分布 $\boldsymbol{w} = (w_1, \cdots, w_n)$, 即给顶点 i 分配满足条件 $\sum_{i=1}^n w_i = 1$ 的数值 $w_i \geqslant 0$. 我们的目标是极大化如下函数:

$$f(\boldsymbol{w}) = \sum_{v_i v_j \in E} w_i w_j.$$

考虑 $\boldsymbol{w}$ 是任意分布, 令 v_i 和 v_j 是分别具有正权重 w_i 和 w_j 的一对不相邻的点. 令 s_i 是 v_i 所有相邻顶点的权重之和, 类似定义 s_j, 且我们可以假设 $s_i \geqslant s_j$. 现在我们将 v_j 的权重给 v_i, 即 v_i 的新权重是 $w_i + w_j$, 同时 v_j 的权重是 0. 对于这个新的概率分布 $\boldsymbol{w}'$ 我们有:

$$f(\boldsymbol{w}') = f(\boldsymbol{w}) + w_j s_i - w_j s_j \geqslant f(\boldsymbol{w}).$$



“移动重物”

我们重复这个过程 (每步减少一个具有正权重的顶点) 直到没有两个不相邻的正权重顶点. 因此我们得出结论, 最优分布是所有非零权重都限制在一个团上 (例如 k- 团) 的分布. 现在如果有$w_1 > w_2 > 0$, 则选择满足 $0 < \varepsilon < w_1 - w_2$ 的 ε 且将 w_1 变成 $w_1 - \varepsilon$, w_2 变成 $w_2 + \varepsilon$. 新得到的分布 $\boldsymbol{w}'$ 满足 $f(\boldsymbol{w}') = f(\boldsymbol{w}) + \varepsilon(w_1 - w_2) - \varepsilon^2 > f(\boldsymbol{w})$, 从而我们可以推断出 $f(\boldsymbol{w})$ 的最大值是在 $w_i = \frac{1}{k}$ 的 k- 团上得到的, 且对于其他点有 $w_i = 0$. 因为一个 k- 团包含 $\frac{k(k-1)}{2}$ 条边, 从而我们得到

$$f(\boldsymbol{w}) = \frac{k(k-1)}{2}\frac{1}{k^2} = \frac{1}{2}\Big(1 - \frac{1}{k}\Big).$$

由于这个表达式是随 k 递增的, 所以我们可以令 $k = p - 1$ (由于 G 没有 p- 团). 因此对于任何 $\boldsymbol{w}$ 我们得到结论

$$f(\boldsymbol{w}) \leqslant \frac{1}{2}\Big(1 - \frac{1}{p-1}\Big).$$

特别地, 当给每个 v_i 赋上权重 $w_i = \frac{1}{n}$ 得到均匀分布时, 这个不等式成立. 因此我们得到

$$\frac{|E|}{n^2} = f\Big(w_i = \frac{1}{n}\Big) \leqslant \frac{1}{2}\Big(1 - \frac{1}{p-1}\Big),$$

上式正是 (1). □

■ **第四个证明.** 这次我们将用到概率论的一些概念. 令 G 是顶点集 $V = \{v_1, \cdots, v_n\}$ 上的任意一个图. 用 d_i 表示 v_i 的度数, 且用 $\omega(G)$ 表示图中最大团的顶点个数, 我们称之为 G 的团数.

断言. 我们有 $\omega(G) \geqslant \displaystyle\sum_{i=1}^n \frac{1}{n - d_i}$.

我们随机地选择顶点集 V 上的置换 $\pi = v_1 v_2 \cdots v_n$, 且每种置换以相同概率 $\frac{1}{n!}$ 出现. 我们考虑以下集合 C_π. v_i 属于 C_π 当且仅当 v_i 与任何满足 $j < i$ 的 v_j 相连. 根据定义, 我们知道 C_π 是 G 中的一个团. 令 $X = |C_\pi|$ 是对应的随机变量. 我们有 $X = \sum_{i=1}^{n} X_i$, 其中 X_i 是顶点 v_i 的指示随机变量, 即当 $v_i \in C_\pi$ 时有 $X_i = 1$, $v_i \notin C_\pi$ 有 $X_i = 0$. 注意到相对于置换 $v_1 v_2 \cdots v_n$ 有 v_i 属于 C_π 当且仅当 v_i 出现在所有不与其相邻的 $n-1-d_i$ 个顶点之前, 换言之, v_i 是 v_i 和与其不相邻的 $n-1-d_i$ 个顶点中的第一个. 这个事件发生的概率是 $\frac{1}{n-d_i}$, 因此 $EX_i = \frac{1}{n-d_i}$.

所以根据期望的线性性, 我们得到

$$E(|C_\pi|) = EX = \sum_{i=1}^{n} EX_i = \sum_{i=1}^{n} \frac{1}{n-d_i}.$$

故至少存在具有这样的基数的团, 我们的断言得证. 为了从该断言推出 Turán 的定理我们运用第 17 章中的 Cauchy-Schwarz 不等式:

$$\Big(\sum_{i=1}^{n} a_i b_i\Big)^2 \leqslant \Big(\sum_{i=1}^{n} a_i^2\Big)\Big(\sum_{n=1}^{n} b_i^2\Big).$$

令 $a_i = \sqrt{n-d_i}$, $b_i = \frac{1}{\sqrt{n-d_i}}$, 则 $a_i b_i = 1$, 因此

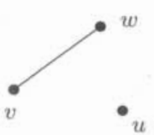
$$n^2 \leqslant \Big(\sum_{i=1}^{n}(n-d_i)\Big)\Big(\sum_{i=1}^{n}\frac{1}{n-d_i}\Big) \leqslant \omega(G)\sum_{i=1}^{n}(n-d_i). \qquad (2)$$

这时, 我们运用 Turán 的假设 $\omega(G) \leqslant p-1$. 同时结合双计数一章中的 $\sum_{i=1}^{n} d_i = 2|E|$, 可由不等式 (2) 推导出

$$n^2 \leqslant (p-1)(n^2 - 2|E|),$$

且这个不等式等价于 Turán 不等式. □

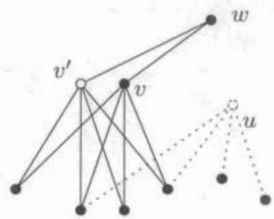
现在我们要介绍第五个证明, 这个证明是这些证明中最漂亮的一个. 它的出处不是很清楚, 我们是从 Stephan Brandt 那里得到的, 而他是在 Oberwolfach 听说的. 由它可以推出一个很强的结论: Turán 图事实上是唯一一个具有最大边数的图. 证明 1 和 2 也可以推出这个更强的结论.



■ **第五个证明.** 令 G 是 n 个顶点上的无 p- 团的边数最多的图.

断言: G 中不包含三个顶点 u, v, w 使得 $vw \in E$, 但 $uv \notin E$, $uw \notin E$.

否则考虑如下情形.



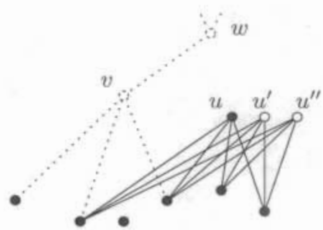
情形 1: $d(u) < d(v)$ 或者 $d(u) < d(w)$.

我们可以假设 $d(u) < d(v)$. 然后我们复制 v, 即构造一个新顶点 v', 它与 v 具有相同的邻居 (但是 vv' 不是一条边), 删去 u, 且保持剩下的不变.

新图 G' 也是无 p- 团的图, 但是对于边数我们有

$$|E(G')| \ = \ |E(G)| + d(v) - d(u) \ > \ |E(G)|,$$

这就产生了矛盾.



情形 2: $d(u) \geqslant d(v)$ 且 $d(u) \geqslant d(w)$.

复制 u 两次且删去 v 和 w (如图所示). 同样新图 G' 没有 p- 团, 且我们计算得到 (结果 -1 是来自边 vw):

$$|E(G')| \ = \ |E(G)| + 2d(u) - (d(v) + d(w) - 1) \ > \ |E(G)|.$$

因此我们再一次推出矛盾.

稍微考虑一下我们就知道断言等价于如下陈述:

$$u \sim v \ :\Longleftrightarrow \ uv \notin E(G)$$

定义了一个等价关系. 因此 G 是一个完全多部图, 即 $G = K_{n_1,\cdots,n_{p-1}}$, 从而定理得证.

参考文献

[1] M. Aigner: *Turán's graph theorem,* Amer. Math. Monthly **102** (1995), 808-816.

[2] N. Alon & J. Spencer: *The Probabilistic Method,* Wiley Interscience 1992.

[3] P. Erdős: *On the graph theorem of Turán (in Hungarian),* Math. Fiz. Lapok **21** (1970), 249-251.

[4] T. S. Motzkin & E. G. Straus: *Maxima for graphs and a new proof of a theorem of Turán,* Canad. J. Math. **17** (1965), 533-540.

[5] P. Turán: *On an extremal problem in graph theory,* Math. Fiz. Lapok **48** (1941), 436-452.



“移动更重的物体”

第 33 章 无差错信息传输

1956 年, 信息论的奠基人 Claude Shannon, 提出了以下非常有趣的问题:

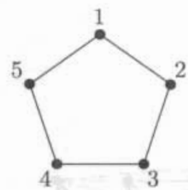
> 假设我们通过信道传送信息给接收者 (有些符号会失真). 使得接收者能够毫无误差地接收到原信息的最大传输率是多少?



Claude Shannon

让我们来看看 Shannon 所提到的"信道"和"传输率". 我们用 V 表示符号集合, 一个信息是由 V 中的一串符号构成的. 我们将信道看成一个图 $G = (V, E)$, 这里 V 是符号组成的集合, E 是由不可靠符号对之间的边构成的集合, 不可靠符号对指的是在传输过程中可能会被混淆的两个符号. 例如, 在电话中传输日常用语时, 我们将符号 B 和 P 联系起来, 因为接收者也许不能辨别它们. 我们称 G 为混淆图.

5-圈图 C_5 将在我们的讨论中起着非常重要的作用. 在这个例子中, 1 和 2 可能会被混淆, 但是 1 和 3 不会, 等等. 理想情况下, 我们想用 5 个符号来传输, 但是因为我们希望传输误差为零, 我们只传输混淆对中的一个符号. 因此对于 5- 圈图, 我们只能用两个符号 (任何不通过边相连的两个符号). 在信息论的语言中, 这意味着对于我们在5-圈图上达到的信息率是 $\log_2 2 = 1$ (而非最大的 $\log_2 5 \approx 2.32$). 显然在这个模型中, 对于任意图 $G = (V, E)$, 我们可以采取的最好方案是从一个最大独立集中传输符号. 因此当传输单个符号时, 信息率是 $\log_2 \alpha(G)$, 其中 $\alpha(G)$ 是 G 的**独立数**.



让我们看看我们是否可以用更大的符号串来代替单个符号以获得更大的信息率. 假设我们要传输长为 2 的符号串. 符号串 u_1u_2 和 v_1v_2 会被混淆当且仅当以下三种情形之一成立:

- $u_1 = v_1$ 且 u_2 会与 v_2 混淆,
- $u_2 = v_2$ 且 u_1 会与 v_1 混淆, 或者
- $u_1 \neq v_1$ 会被混淆且 $u_2 \neq v_2$ 会被混淆.

用图论中的语言, 这相当于考虑两个图 $G_1=(V_1,E_1)$ 和 $G_2=(V_2,E_2)$ 的乘积 $G_1\times G_2$. 乘积 $G_1\times G_2$ 有顶点集 $V_1\times V_2=\{(u_1,u_2):u_1\in V_1,u_2\in V_2\}$, 且 $(u_1,u_2)\neq(v_1,v_2)$ 是通过边相连的当且仅当对于 $i=1,2$ 有$u_i=v_i$ 或者 $u_iv_i\in E_i$. 因此符号串长为 2 的混淆图是单符号混淆图 G 与自身的乘积图 $G^2=G\times G$. 则对于符号串长为 2 的情形, 每个符号的信息率是:

$$\frac{\log_2\alpha(G^2)}{2} \;=\; \log_2\sqrt{\alpha(G^2)}.$$

现在我们用任意长度的符号串 n, 混淆图是 $G^n=G\times G\times\cdots\times G$, 其顶点集为 $V^n=\{(u_1,\cdots,u_n):u_i\in V\}$, 且 $(u_1,\cdots,u_n)\neq(v_1,\cdots v_n)$ 通过边相连当且仅当对于任意 i 有 $u_i=v_i$ 或 $u_iv_i\in E$ 成立. 在符号串长度为 n 的情形下, 每个符号的信息率为:

$$\frac{\log_2\alpha(G^n)}{n} \;=\; \log_2\sqrt[n]{\alpha(G^n)}.$$

我们可以对 $\alpha(G^n)$ 说些什么呢? 这里是第一个观察. 令 $U\subseteq V$ 是 G 中最大的独立集, 且 $|U|=\alpha$. G^n 中具有形式 $(u_1,\cdots,u_n)$ (对于任意 i, $u_i\in U$) 的 α^n 个顶点, 显然形成了 G^n 中的独立集. 因此,

$$\alpha(G^n) \;\geqslant\; \alpha(G)^n,$$

从而

$$\sqrt[n]{\alpha(G^n)} \;\geqslant\; \alpha(G),$$

这意味着通过用更长的符号串来代替单个符号, 我们不可能降低信息率. 顺便提及一下, 这是编码理论的一个基本思想: 通过用更长的串来编码符号, 会使无差错传输更加有效.

不考虑对数, 我们得到 Shannon 的基本定义: 图G 的**无差错容量**是如下定义的:

$$\Theta(G) := \sup_{n\geqslant1}\sqrt[n]{\alpha(G^n)},$$

Shannon 的问题就是计算 $\Theta(G)$, 特别是计算 $\Theta(C_5)$.

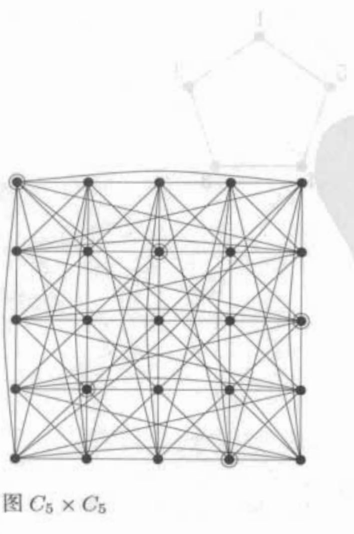


图 $C_5\times C_5$

让我们看看 C_5. 至今我们知道 $\alpha(C_5)=2\leqslant\Theta(C_5)$. 让我们看看之前所描述的 5- 圈图, 或者画在边栏的乘积图 $C_5\times C_5$, 我们知道 $\{(1,1),(2,3),(3,5),(4,2),(5,4)\}$ 是 ${C_5}^2$ 的独立集. 因此我们有 $\alpha({C_5}^2)\geqslant5$. 因为一个独立集只能包含来自连续两行的两个顶点, 我们得到 $\alpha({C_5}^2)=5$. 因此, 通过运用长为 2 的符号串, 我们把容量的下界增加到 $\Theta(C_5)\geqslant\sqrt{5}$.

至今我们没有给出容量的上界. 为了得到这个上界, 我们又一次运用 Shannon 原始的思想. 首先, 我们需要用到独立集的对偶定义. 我们回忆一下: 一个子集 $C \subseteq V$ 称为一个团, 如果 C 中的任何两个顶点都是有边相连的. 因此顶点是基数为 1 的平凡团, 边是基数为 2 的团, 三角形是基数为 3 的团, 等等. 令 $\mathcal{C}$ 是 G 中团的集合. 考虑顶点集上的任一概率分布 $\boldsymbol{x} = (x_v : v \in V)$, 即 $x_v \geqslant 0$ 且 $\sum_{v\in V} x_v = 1$. 对于任意概率分布 $\boldsymbol{x}$, 我们将其与"最大团值"联系起来:

$$\lambda(\boldsymbol{x}) = \max_{C\in\mathcal{C}} \sum_{v\in C} x_v,$$

最后我们令

$$\lambda(G) = \min_{\boldsymbol{x}} \lambda(\boldsymbol{x}) = \min_{\boldsymbol{x}} \max_{C\in\mathcal{C}} \sum_{v\in C} x_v.$$

为了精确, 我们应该用 inf 代替 min, 但是最小值是存在的, 这是因为 $\lambda(\boldsymbol{x})$ 在所有分布构成的紧集上是连续的.

现在考虑一个 V 的极大独立集 U, 其基数 $\alpha(G) = \alpha$. 对于 U 我们定义概率分布 $\boldsymbol{x}_U = (x_v : v \in V)$: 对于 $v \in U$ 我们有 $x_v = \frac{1}{\alpha}$, 否则 $x_v = 0$. 因为任何一个团至多包含一个 U 中的顶点, 我们推出 $\lambda(\boldsymbol{x}_U) = \frac{1}{\alpha}$, 且通过 $\lambda(G)$ 的定义我们有:

$$\lambda(G) \leqslant \frac{1}{\alpha(G)} \quad \text{或者} \quad \alpha(G) \leqslant \lambda(G)^{-1}.$$

事实上, Shannon 所观察到 $\lambda(G)^{-1}$ 是所有 $\sqrt[n]{\alpha(G^n)}$ 的一个上界, 因此它也是 $\Theta(G)$ 的一个上界. 为了证明这个结论, 我们只需证明对于图 G, H 有

$$\lambda(G \times H) = \lambda(G)\lambda(H). \tag{1}$$

由此可以导出 $\lambda(G^n) = \lambda(G)^n$ 且

$$\begin{aligned} \alpha(G^n) &\leqslant \lambda(G^n)^{-1} = \lambda(G)^{-n} \\ \sqrt[n]{\alpha(G^n)} &\leqslant \lambda(G)^{-1}. \end{aligned}$$

为了证明 (1), 我们将运用线性规划的对偶性原理 (参见 [1]), 于是得到

$$\lambda(G) = \min_{\boldsymbol{x}} \max_{C\in\mathcal{C}} \sum_{v\in C} x_v = \max_{\boldsymbol{y}} \min_{v\in V} \sum_{C\ni v} y_C, \tag{2}$$

其中等式的右边跑遍了 $\mathcal{C}$ 上的所有概率分布 $\boldsymbol{y} = (y_C : C \in \mathcal{C})$.

考虑 $G \times H$, 且令 $\boldsymbol{x}$ 和 $\boldsymbol{x}'$ 是达到最小值的分布, 即 $\lambda(\boldsymbol{x}) = \lambda(G)$, $\lambda(\boldsymbol{x}') = \lambda(H)$. 在 $G \times H$ 的顶点集中, 我们对顶点 (u, v) 分配数值 $z_{(u,v)} = x_u x'_v$. 由于 $\sum_{(u,v)} z_{(u,v)} = \sum_u x_u \sum_v x'_v = 1$, 我们得到一个概率分布. 我们观察到 $G \times H$ 中的最大团具有形式 $C \times D = \{(u, v) : u \in C, v \in D\}$, 其中 C 和 D 分别是 G 和 H 中的团. 因此根据 $\lambda(G \times H)$ 的定义我们得到

$$\begin{aligned}\lambda(G \times H) \leqslant \lambda(\boldsymbol{z}) &= \max_{C \times D} \sum_{(u,v) \in C \times D} z_{(u,v)} \\ &= \max_{C \times D} \sum_{u \in C} x_u \sum_{v \in D} x'_v = \lambda(G)\lambda(H).\end{aligned}$$

同样地, 我们将用 (2) 中 $\lambda(G)$ 的对偶表达式来证明反过来的不等式 $\lambda(G \times H) \geqslant \lambda(G)\lambda(H)$. 总之, 对于任何图 G, 我们有:

$$\Theta(G) \leqslant \lambda(G)^{-1}.$$

让我们将结果运用到 5- 圈图或更一般的 m-圈图 C_m 上. 通过运用顶点上的均匀分布 $(\frac{1}{m}, \cdots, \frac{1}{m})$, 我们得到 $\lambda(C_m) \leqslant \frac{2}{m}$, 这是因为任何团至多包含两个顶点. 相似地, 我们分配 $\frac{1}{m}$ 给边以及 0 给这些顶点, 通过 (2) 的对偶表达式我们有 $\lambda(C_m) \geqslant \frac{2}{m}$. 我们得到结论 $\lambda(C_m) = \frac{2}{m}$, 且对于任何 m 有以下式子成立:

$$\Theta(C_m) \leqslant \frac{m}{2}.$$

如果 m 是偶数, 则显然地有 $\alpha(C_m) = \frac{m}{2}$, 故 $\Theta(C_m) = \frac{m}{2}$. 但是, 如果 m 是奇数, 我们有 $\alpha(C_m) = \frac{m-1}{2}$. 对于 $m = 3$, C_3 是一个团, 且每个乘积 C_3^n 也是团, 这就蕴含了 $\alpha(C_3) = \Theta(C_3) = 1$. 因此, 对于我们最感兴趣的5- 圈图, 我们到目前为止知道:

$$\sqrt{5} \leqslant \Theta(C_5) \leqslant \frac{5}{2}. \tag{3}$$

通过运用线性规划的方法 (还有其他一些思想) , Shannon 计算出了许多图的容量, 特别是所有顶点数是五或比五少的图, 但除了 C_5 之外, 他不能把 (3) 式的上界降低. 在 20 年之后, László Lovász 用一个极其简单的论证证明了 $\Theta(C_5) = \sqrt{5}$, 从而给看似复杂的组合问题提供了一个出乎意料且漂亮的解.



Lovász 伞

Lovász 的主要新思想是用长度为 1 的实值向量来表示顶点 v, 且两个顶点不相邻当且仅当表示它们的向量正交. 我们称这样的向量集为 G 的正交表现. 显然, 这样一个表现总是存在的: 只要选择 $m =$

$|V|$ 维空间的单位向量: $(1,0,\cdots,0)^T,(0,1,0,\cdots,0)^T,\cdots,(0,0,\cdots,1)^T$.

对于图 C_5, 通过考虑具有五根长度为 1 的伞骨 $\boldsymbol{v}_1,\cdots,\boldsymbol{v}_5$ 的"伞", 我们可以得到 C_5 在 $\mathbb{R}^3$ 中的正交表现. 现在打开伞(伞顶在原点) 直至交错的伞骨之间的夹角是 90°.

Lovász 接下来对于伞高 h, 即 $\mathbf{0}$ 和 S 之间的距离, 提供了上界:

$$\Theta(C_5) \leqslant \frac{1}{h^2}. \tag{4}$$

参看下面两个方框里的内容, 通过一个简单的运算我们得到 $h^2=\frac{1}{\sqrt{5}}$. 从而 $\Theta(C_5)\leqslant\sqrt{5}$, 因此 $\Theta(C_5)=\sqrt{5}$.

让我们看看 Lovász 是如何证明不等式 (4) 的. (事实上, 他的结果更具一般性.) 考虑两个向量 $\boldsymbol{x}=(x_1,\cdots,x_s)$, $\boldsymbol{y}=(y_1,\cdots,y_s)$ 在 $\mathbb{R}^s$ 中的内积

$$\langle \boldsymbol{x},\boldsymbol{y}\rangle = x_1y_1+\cdots+x_sy_s,$$

则 $|\boldsymbol{x}|^2=\langle \boldsymbol{x},\boldsymbol{x}\rangle=x_1^2+\cdots+x_s^2$ 是向量 $\boldsymbol{x}$ 长度 $|\boldsymbol{x}|$ 的平方, 且 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的夹角 γ 是

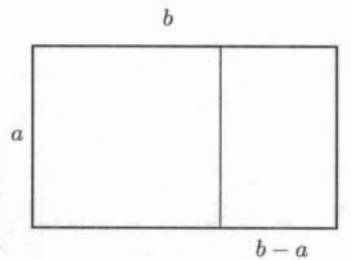
$$\cos\gamma = \frac{\langle \boldsymbol{x},\boldsymbol{y}\rangle}{|\boldsymbol{x}||\boldsymbol{y}|}.$$

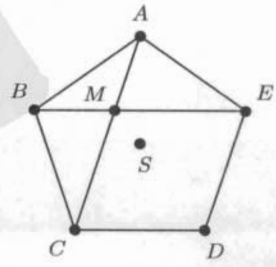
因此 $\langle \boldsymbol{x},\boldsymbol{y}\rangle=0$ 当且仅当 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是正交的.

五边形和黄金分割

如果一个矩形切掉一个长为 a 的正方形之后剩下的矩形与原矩形具有相同的形状, 那么传统上认为这样的矩形很美观. 这样的矩形的两条边 a,b 必须满足 $\frac{b}{a}=\frac{a}{b-a}$. 设比例为 $\tau:=\frac{b}{a}$, 我们得到 $\tau=\frac{1}{\tau-1}$ 或者 $\tau^2-\tau-1=0$. 解这个二次方程我们得到黄金分割 $\tau=\frac{1+\sqrt{5}}{2}\approx 1.6180$.

现在我们考虑边长为 a 的正五边形, 且设 d 为其对角线长. Euclid 已经知道 (Book XIII,8) $\frac{d}{a}=\tau$, 且两条对角线的交点是对角线的黄金分割点.





以下是 Euclid 书中的证明. 因为正五边形的内角之和是 3π, 所以任何一个内角为 $\frac{3\pi}{5}$. 因为 ABE 是等腰三角形, 故 $\sphericalangle ABE = \frac{\pi}{5}$. 这也蕴含了 $\sphericalangle AMB = \frac{3\pi}{5}$, 且我们得到三角形 ABC 和 AMB 是相似的. 四边形 $CMED$ 是菱形, 因为它的对边还是平行的 (通过角的度数可知), 由此得到 $|MC| = a$ 以及 $|AM| = d - a$. 根据 ABC 和 AMB 的相似性, 我们有

$$\frac{d}{a} = \frac{|AC|}{|AB|} = \frac{|AB|}{|AM|} = \frac{a}{d-a} = \frac{|MC|}{|MA|} = \tau.$$

还有其他结论. 例如 s 是五边形 S 顶点到中心的距离, 请读者证明关系式 $s^2 = \frac{d^2}{\tau+2}$ (注意到 BS 将对角线 AC 平分).

为了结束我们的几何之旅, 现在考虑具有顶部是正则五边形的伞. 因为相互交错的伞骨 (长为 1) 形成了一个直角, Pythagoras 定理告诉我们 $d = \sqrt{2}$, 因此 $s^2 = \frac{2}{\tau+2} = \frac{4}{\sqrt{5}+5}$. 再一次运用 Pythagoras 定理, 我们得到所要求的高度值 $h = |OS|$:

$$h^2 = 1 - s^2 = \frac{1+\sqrt{5}}{\sqrt{5}+5} = \frac{1}{\sqrt{5}}.$$

现在我们来求上界"$\Theta(G) \leqslant \sigma_T^{-1}$". 它对于任何图 G 的 Shannon 容量都有一个非常"好"的正交表现. 设 $T = \{\boldsymbol{v}^{(1)}, \cdots, \boldsymbol{v}^{(m)}\}$ 是图 G 在 $\mathbb{R}^s$ 中的正交表现, 其中 $\boldsymbol{v}^{(i)}$ 对应着顶点 v_i. 此外, 我们假设所有向量 $\boldsymbol{v}^{(i)}$ 与向量$\boldsymbol{u} := \frac{1}{m}(\boldsymbol{v}^{(1)} + \cdots + \boldsymbol{v}^{(m)})$有相同的夹角 ($\neq 90°$), 或者等价地, 对于任何 i, 内积

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle = \sigma_T$$

有相同的值且 $\sigma_T \neq 0$. 我们称 σ_T 是表现 T 的常数. 对于 Lovász 伞, C_5 的表现显然满足条件 $\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle = \sigma_T$, 其中 $\boldsymbol{u} = \vec{OS}$.

现在我们按如下三步展开.

(A) 考虑 V 上的概率分布 $\boldsymbol{x} = (x_1, \cdots, x_m)$ 且令

$$\mu(\boldsymbol{x}) := |x_1 \boldsymbol{v}^{(1)} + \cdots + x_m \boldsymbol{v}^{(m)}|^2,$$

以及

$$\mu_T(G) := \inf_{\boldsymbol{x}} \mu(\boldsymbol{x}).$$

令 U 是 G 中基数为 $|U| = \alpha$ 的最大独立集, 并且定义 $\boldsymbol{x}_U = (x_1, \cdots, x_m)$, 其中如果 $v_i \in U$, 则 $x_i = \frac{1}{\alpha}$, 否则 $x_i = 0$. 由于所有的向量 $\boldsymbol{v}^{(i)}$ 都是单位长度的且对于任何两个不相邻的顶点 $\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(j)} \rangle = 0$, 我们推断出

$$\mu_T(G) \leqslant \mu(\boldsymbol{x}_U) = \Big| \sum_{i=1}^{m} x_i \boldsymbol{v}^{(i)} \Big|^2 = \sum_{i=1}^{m} x_i^2 = \alpha \frac{1}{\alpha^2} = \frac{1}{\alpha}.$$

因此我们有 $\mu_T(G) \leqslant \alpha^{-1}$, 并且

$$\alpha(G) \leqslant \frac{1}{\mu_T(G)}.$$

(B) 接下来我们计算 $\mu_T(G)$. 我们需要 Cauchy-Schwarz 不等式

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle^2 \leqslant |\boldsymbol{a}|^2 \, |\boldsymbol{b}|^2$$

其中向量 $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^s$. 将其运用到 $\boldsymbol{a} = x_1 \boldsymbol{v}^{(1)} + \cdots + x_m \boldsymbol{v}^{(m)}$ 和 $\boldsymbol{b} = \boldsymbol{u}$ 上, 则得到

$$\langle x_1 \boldsymbol{v}^{(1)} + \cdots + x_m \boldsymbol{v}^{(m)}, \boldsymbol{u} \rangle^2 \leqslant \mu(\boldsymbol{x}) \, |\boldsymbol{u}|^2. \tag{5}$$

根据我们的假设, 对于任意的 i 有 $\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle = \sigma_T$, 对于任何概率分布 $\boldsymbol{x}$, 我们得到

$$\langle x_1 \boldsymbol{v}^{(1)} + \cdots + x_m \boldsymbol{v}^{(m)}, \boldsymbol{u} \rangle = (x_1 + \cdots + x_m) \, \sigma_T = \sigma_T.$$

因此, 特别地, 这对于均匀分布 $(\frac{1}{m}, \cdots, \frac{1}{m})$ 也成立, 这就蕴含了 $|\boldsymbol{u}|^2 = \sigma_T$. 因此 (5) 就变成:

$$\sigma_T^2 \leqslant \mu(\boldsymbol{x}) \, \sigma_T \quad \text{或者} \quad \mu_T(G) \geqslant \sigma_T.$$

另一方面, 对于 $\boldsymbol{x} = (\frac{1}{m}, \cdots, \frac{1}{m})$ 我们得到

$$\mu_T(G) \leqslant \mu(\boldsymbol{x}) = |\tfrac{1}{m}(\boldsymbol{v}^{(1)} + \cdots + \boldsymbol{v}^{(m)})|^2 = |\boldsymbol{u}|^2 = \sigma_T,$$

因此我们证明了

$$\mu_T(G) = \sigma_T. \tag{6}$$

总之, 我们给常数为 σ_T 的任意正交表现 T 建立了不等式

$$\alpha(G) \leqslant \frac{1}{\sigma_T}. \tag{7}$$

(C) 为了将不等式扩充到 $\Theta(G)$ 上, 我们像以前一样来讨论. 再

一次考虑两个图的乘积 $G\times H$. 令 G 和 H 的正交表现分别是 $\mathbb{R}^r$ 中的常数为 σ_R 的 R 和 $\mathbb{R}^s$ 中的常数为 σ_S 的 S. 令 $\boldsymbol{v}=(v_1,\cdots,v_r)$ 是 R 中的一个向量, $\boldsymbol{w}=(w_1,\cdots,w_s)$ 是 S 中的一个向量. 图 $G\times H$ 中的顶点对应于向量对 $(\boldsymbol{v},\boldsymbol{w})$, 我们将其与如下向量联系起来:

$$\boldsymbol{v}\boldsymbol{w}^T:=(v_1w_1,\cdots,v_1w_s,v_2w_1,\cdots,v_2w_s,\cdots,v_rw_1,\cdots,v_rw_s)\in\mathbb{R}^{rs}.$$

很容易验证 $R\times S:=\{\boldsymbol{v}\boldsymbol{w}^T:\boldsymbol{v}\in R,\boldsymbol{w}\in S\}$ 是图 $G\times H$ 中常数为 $\sigma_R\sigma_S$ 的正交表现. 根据 (6) 我们得到

$$\mu_{R\times S}(G\times H)=\mu_R(G)\mu_S(H).$$



"有五根伞骨的伞"

对于图 $G^n=G\times\cdots\times G$ 以及其常数为 σ_T 的表现 T, 这表明

$$\mu_{T^n}(G^n)=\mu_T(G)^n=\sigma_T^n,$$

根据 (7) 我们得到

$$\alpha(G^n)\leqslant\sigma_T^{-n},\qquad\sqrt[n]{\alpha(G^n)}\leqslant\sigma_T^{-1}.$$

综合上述讨论我们完成了 Lovász 定理的论证:

定理. 当 $T=\{\boldsymbol{v}^{(1)},\cdots,\boldsymbol{v}^{(m)}\}$ 是图 G 的常数为 σ_T 的正交表现时, 有

$$\Theta(G)\leqslant\frac{1}{\sigma_T}.\tag{8}$$

看看 Lovász 伞, 我们有 $\boldsymbol{u}=(0,0,h=\frac{1}{\sqrt[4]{5}})^T$, 故得到 $\sigma=\langle\boldsymbol{v}^{(i)},\boldsymbol{u}\rangle=h^2=\frac{1}{\sqrt{5}}$, 这蕴含着 $\Theta(C_5)\leqslant\sqrt{5}$. 因此 Shannon 的问题解决了.

让我们继续我们的讨论. 从 (8) 中我们看出 G 的一个表现的 σ_T 越大, 我们得到 $\Theta(G)$ 的上界越好. 下面给出了我们得到任何图 G 的一个正交表现的方法. 我们将 $G=(V,E)$ 与如下定义的邻接矩阵 $A=(a_{ij})$ 联系起来: 设顶点集为 $V=\{v_1,\cdots,v_m\}$, 则我们令

$$a_{ij}:=\begin{cases}1 & 若\ v_iv_j\in E\\ 0 & 否则,\end{cases}$$

$$A=\begin{pmatrix}0&1&0&0&1\\1&0&1&0&0\\0&1&0&1&0\\0&0&1&0&1\\1&0&0&1&0\end{pmatrix}$$

5-圈图 C_5 的邻接矩阵

A 是主对角线为 0 的实对称矩阵.

现在我们需要来自线性代数的两个事实. 第一, 作为一个对称矩阵 A 有 m 个实特征值 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_m$ (其中的有些是相等的), 并且这些特征值的和是和 A 的主对角线上的元素之和相等的,

即为 0. 因此, 最小的特征值一定是负的 (除非当 G 是无边图时平凡情况) . 令 $p = |\lambda_m| = -\lambda_m$ 是最小特征值的绝对值, 考虑矩阵

$$M \ := \ I + \frac{1}{p}A,$$

其中 I 表示 $(m \times m)$ 阶单位矩阵. 这个 M 的特征值是 $1 + \frac{\lambda_1}{p} \geqslant 1 + \frac{\lambda_2}{p} \geqslant \cdots \geqslant 1 + \frac{\lambda_m}{p} = 0$. 现在我们来引用第二个结果(线性代数中的主轴定理): 如果 $M = (m_{ij})$ 是所有特征值大于等于零的实对称矩阵, 则对于 $s = \text{rank}(M)$ 有向量 $\boldsymbol{v}^{(1)}, \cdots, \boldsymbol{v}^{(m)} \in \mathbb{R}^s$ 使得

$$m_{ij} \ = \ \langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(j)} \rangle \qquad (1 \leqslant i, j \leqslant m).$$

特别地, 对于 $M = I + \frac{1}{p}A$ 我们得到

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(i)} \rangle \ = \ m_{ii} = 1 \qquad \text{对于任意 } i$$

和

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(j)} \rangle \ = \ \frac{1}{p}a_{ij} \qquad \text{对于 } i \neq j.$$

由于对于任意 $v_iv_j \notin E$ 有 $a_{ij} = 0$, 我们得到向量 $\boldsymbol{v}^{(1)}, \cdots, \boldsymbol{v}^{(m)}$ 确实形成 G 的一个正交表现.

最后, 让我们把这个构造运用到 m- 圈图 C_m 上 (其中 $m \geqslant 5$ 是奇数) . 这里我们很容易计算 $p = |\lambda_{\min}| = 2\cos\frac{\pi}{m}$ (见方框).

C_m 的特征值

考虑C_m的邻接矩阵A. 为了得到其特征值(特征向量), 我们运用 1 的 m 次单位根. 它们是 $1, \zeta, \zeta^2, \cdots, \zeta^{m-1}$, 其中 $\zeta = e^{\frac{2\pi i}{m}}$ (见第5 章方框).

令 $\lambda = \zeta^k$ 是这些根中的任意一个, 则我们称 $(1, \lambda, \lambda^2, \cdots, \lambda^{m-1})^T$ 是 A 的关于特征值 $\lambda + \lambda^{-1}$ 的特征向量. 事实上, 根据 A 的结构我们知道

$$A \begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{m-1} \end{pmatrix} = \begin{pmatrix} \lambda & + & \lambda^{m-1} \\ \lambda^2 & + & 1 \\ \lambda^3 & + & \lambda \\ & \vdots & \\ 1 & + & \lambda^{m-2} \end{pmatrix} = (\lambda + \lambda^{-1}) \begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{m-1} \end{pmatrix}.$$

由于特征向量 $(1, \lambda, \cdots, \lambda^{m-1})$ 是相互独立的 (它们形成了一个 Vandermonde 矩阵), 我们得到对于奇数 m,

$$\begin{aligned}\zeta^k + \zeta^{-k} &= [(\cos(2k\pi/m) + i\sin(2k\pi/m)] \\ &\quad + [\cos(2k\pi/m) - i\sin(2k\pi/m)] \\ &= 2\cos(2k\pi/m) \qquad (0 \leqslant k \leqslant \tfrac{m-1}{2})\end{aligned}$$

都是 A 的特征值. 由于余弦函数是递减函数, 故

$$2\cos\left(\frac{(m-1)\pi}{m}\right) = -2\cos\frac{\pi}{m}$$

是 A 的最小特征值.

邻接矩阵的每一行包括两个 1, 这蕴含着矩阵M 每一行的行和为 $1+\frac{2}{p}$. 对于表现 $\{\boldsymbol{v}^{(1)}, \cdots, \boldsymbol{v}^{(m)}\}$, 这意味着

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(1)} + \cdots + \boldsymbol{v}^{(m)} \rangle = 1 + \frac{2}{p} = 1 + \frac{1}{\cos\frac{\pi}{m}},$$

故对于任意 i 有

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle = \frac{1}{m}(1 + (\cos\tfrac{\pi}{m})^{-1}) = \sigma.$$

因此, 我们运用我们的主要结果 (8), 得到结论:

$$\Theta(C_m) \leqslant \frac{m}{1 + (\cos\frac{\pi}{m})^{-1}} \quad (\text{对于奇数 } m \geqslant 5). \tag{9}$$

注意到由于 $\cos\frac{\pi}{m} < 1$, (9) 的上界比之前我们找到的上界 $\Theta(C_m) \leqslant \frac{m}{2}$ 更好. 更多地, $\cos\frac{\pi}{5} = \frac{\tau}{2}$, 其中 $\tau = \frac{\sqrt{5}+1}{2}$ 是黄金分割. 因此对于 $m = 5$, 我们又一次得到

$$\Theta(C_5) \leqslant \frac{5}{1 + \frac{4}{\sqrt{5}+1}} = \frac{5(\sqrt{5}+1)}{5+\sqrt{5}} = \sqrt{5}.$$

由这个构造所产生的正交表现当然就是 "Lovász 伞".

那么关于 C_7, C_9, 以及其他奇圈图呢? 通过考虑 $\alpha(C_m^2), \alpha(C_m^3)$ 以及其他小的幂, 下界 $\frac{m-1}{2} \leqslant \Theta(C_m)$ 显然可以增加, 但是对于 $m \geqslant 7$ 的奇数我们知道的最好的下界和 (8) 的上界是不一致的. 因此, 在 Lovász 精彩地证明了 $\Theta(C_5) = \sqrt{5}$ 之后的20年, 这些问题仍然没

例如, 对于 $m = 7$, 我们知道 $\sqrt[4]{108} \leqslant \Theta(C_7) \leqslant \frac{7}{1+(\cos\frac{\pi}{7})^{-1}}$, 即 $3.2237 \leqslant \Theta(C_7) \leqslant 3.3177$.

有解决且被看成是非常难的问题——但是毕竟我们之前也有过这种情形.

参考文献

[1] V. Chvátal: *Linear Programming,* Freeman, New York 1983.

[2] W. Haemers: *Eigenvalue methods,* in: "Packing and Covering in Combinatorics" (A. Schrijver, ed.), Math. Centre Tracts **106** (1979), 15-38.

[3] L. Lovász: *On the Shannon capacity of a graph,* IEEE Trans. Information Theory **25** (1979), 1-7.

[4] C. E. Shannon: *The zero-error capacity of a noisy channel,* IRE Trans. Information Theory **3** (1956), 3-15.

朋友圈与交际花

第 34 章



"交际花的微笑"

以下这个问题到底是谁最先提出和深入探究的已经无从考证.这个问题就是:

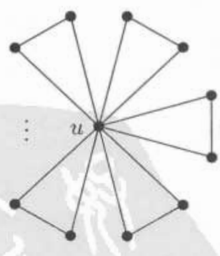
> *假设在一群人当中任意两个人都恰好有一个共同的朋友. 那么总有一个人(我们称之为交际花)是所有人的朋友.*

用数学的专业语言来表达,这就是友谊定理.

在纠缠于证明之前让我们先用图论的语言来重述一下这个问题.我们把人看成是图上的顶点,如果两个人是朋友,那么就在代表他们的两顶点之间联上一条边. 我们默认友谊都是相互的,也就是说,如果 u 是 v 的朋友,那么 v 也是 u 的朋友,并且每个人都不是自己的朋友.因而定理变成了以下的形式:

定理. *假设 G 是一个有限图,其中任意两个顶点都恰好有一个共同的邻居,那么必然存在一个顶点是跟其他所有顶点都相连.*

注意这样的有限图是存在的,参看边图,图中的u 是交际花.然而,这类"风车图"实际上是唯一拥有这种性质的图. 事实上,不难证明在交际花存在的情况下只有这种"风车图"是唯一可能的.



风车图

令人惊奇的是,友谊定理对无限图并不成立!事实上,要构造一个递归的反例,可以从一个五边形开始,然后不停地为没有共同邻居的顶点添加共同邻居.这样将会得到一个(可数的)无限的没有交际花的友谊图.

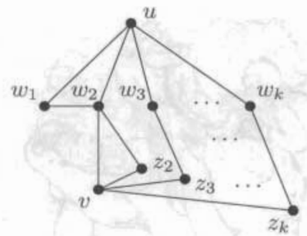
关于友谊定理有几个证明,但是由 Paul Erdős, Alfred Rényi 和 Vera Sós 给出的第一个证明一直是最完善的.

■ **证明.** 假设断言是错误的,而 G 是一个反例,也就是说,没有哪个 G 的顶点是跟其他所有的顶点是相连的. 为了得到矛盾我们分两步走.第一部分是组合,第二部分是线性代数.



(1) 我们断言 G 是一个正则图, 也就是说, 对任何的 $u, v \in V$, $d(u) = d(v)$. 首先注意到定理中的条件能推出在 G 中没有长度为 4 的圈. 我们将这个条件称为C_4- 条件.

我们首先证明任意两个不相连的顶点 u 和 v 有同样的度 $d(u) = d(v)$. 假设 $d(u) = k$, 而 $w_1, \cdots, w_k$ 是 u 的邻居. w_i 中恰好有一个, 比如 w_2 是与 v 相连的, 而 w_2 恰好与其他的 w_i 中的一个相连, 比如 w_1, 由此我们得到了如边栏所示的图. 顶点 v 和 w_1 有共同的邻居 w_2, 而与 w_i $(i \geqslant 2)$ 有一个共同的邻居 z_i $(i \geqslant 2)$. 由 C_4- 条件, 所有这些 z_i 都是不同的. 所以, $d(v) \geqslant k = d(u)$, 从而由对称性 $d(u) = d(v) = k$.



为了完成(1)的证明, 观察到任何不同于 w_2 的顶点是不与 u 或 v 相连的, 所以度数为 k, 而这个我们已经证明. 但是因为 w_2 也有个不相邻的点, 它度数也为 k, 所以 G 是 k- 正则的.

对 u 的所有 k 个邻居的度数求和我们得到 k^2. 因为任意一个顶点 (除了 u) 与 u 都恰好有一个共同的邻居, 我们对每个顶点都做了一次计数, 除了 u, 它被数了 k 次. 所以 G 总共的顶点数为

$$n = k^2 - k + 1. \tag{1}$$

(2) 剩下的证明是对线性代数的一些标准结果的漂亮应用. 首先注意 k 一定比 2 大, 因为由 (1) 对 $k \leqslant 2$ 只可能有 $G = K_1$ 和 $G = K_3$, 而它们都是平凡的风车图. 考虑其邻接矩阵 $A = (a_{ij})$, 如上一章所定义的. 由(1), 矩阵中任意一行都恰好有 k 个 1, 且由定理的条件, 对任意两行都恰好有一列其中的元素都是 1. 另外注意到主对角线是由 0 组成的. 因此我们有

$$A^2 = \begin{pmatrix} k & 1 & \cdots & 1 \\ 1 & k & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & k \end{pmatrix} = (k-1)I + J,$$

其中 I 是单位矩阵, 而 J 是全 1 阵. 立刻可以验证 J 有特征值 n (重数为 1) 以及 0 (重数为 $n-1$). 由此可得 A^2 有特征值 $k - 1 + n = k^2$ (重数为 1) 和 $k-1$ (重数为 $n-1$).

因为 A 是对称的而可对角化, 所以 A 有特征值 k (重数为 1) 以及 $\pm\sqrt{k-1}$. 假设特征值中的 r 个等于 $\sqrt{k-1}$, s 个等于 $-\sqrt{k-1}$, 而 $r + s = n - 1$. 现在我们快要完成了. 因为 A 中的特征值之和即

为其迹 (而这个数值为 0), 我们发现:

$$k + r\sqrt{k-1} - s\sqrt{k-1} \;=\; 0,$$

并且特别地, $r \neq s$,

$$\sqrt{k-1} \;=\; \frac{k}{s-r}.$$

而如果一个自然数 m 的平方根 $\sqrt{m}$ 是有理数, 那么它就是一个整数! 这个定理的优雅的证明是 Dedekind 在 1858 年提供的: 令 n_0 是满足 $n_0\sqrt{m} \in \mathbb{N}$ 的最小自然数. 如果 $\sqrt{m} \notin \mathbb{N}$, 那么存在 $\ell \in \mathbb{N}$ 使得 $0 < \sqrt{m} - \ell < 1$. 设 $n_1 := n_0(\sqrt{m} - \ell)$, 我们发现 $n_1 \in \mathbb{N}$ 以及 $n_1\sqrt{m} = n_0(\sqrt{m}-\ell)\sqrt{m} = n_0 m - \ell(n_0\sqrt{m}) \in \mathbb{N}$. 而由于 $n_1 < n_0$, 这与 n_0 的最小性矛盾.

回到我们的方程, 让我们设 $h = \sqrt{k-1} \in \mathbb{N}$, 那么

$$h(s-r) \;=\; k \;=\; h^2 + 1.$$

因为 h 整除 $h^2 + 1$ 和 h^2, 我们发现 h 必须等于 1, 于是 $k = 2$, 而我们已经排除了这种情况. 所以我们得到了矛盾, 从而完成证明. □

但是故事并没有到这里就结束. 让我们再按照以下的方式来重述我们的问题: 假设 G 是一个图, 在图中任意两个顶点都会恰好有一条长度为 2 的路. 显然, 这是友谊条件的等价形式. 我们的定理说的就是只有风车图才能满足以上条件. 但如果我们考虑长度大于 2 的路又如何呢? 一个源自 Anton Kotzig 的猜想断言类似的情况是不可能的.

Kotzig 猜想. *令 $\ell > 2$. 那么不存在这样的有限图, 使得任意两个顶点间恰好有一条长度为 ℓ 的路.*

Kotzig 自己证明了在 $\ell \leqslant 8$ 的情况下这个猜想的正确性. 在 [3] 中, $\ell = 20$ 的情形被证明了, 并且 A. Kostochka 最近告诉我们现在 $\ell \leqslant 33$ 的情况都被证明了. 然而, 一个更一般的证明似乎难以获得……

参考文献

[1] P. Erdős, A. Rényi, & V. Sós: *On a problem of graph theory,* Studia Sci. Math. **1** (1966), 215-235.

[2] A. Kotzig: *Regularly k-path connected graphs,* Congressus Numerantium **40** (1983), 137-141.

[3] A. Kostochka: *The nonexistence of certain generalized friendship graphs,* in: "Combinatorics" (Eger, 1987), Colloq. Math. Soc. János Bolyai **52**, North-Holland, Amsterdam 1988, 341-356.

概率 (有时) 让计数变得简单 第 35 章

就像我们用 Paul Erdős 的几篇早期的数论文章来开始本书的一样, 我们在最后来讨论可能被认为是他影响最深远的精神遗产——他与 Alfred Rényi 一同引入的概率方法. 以最简单的方式来说就是:

> 如果在一个事件集中, 不具有某种特定性质的事件的并的概率小于 1, 那么一定存在某个事件是有这种性质的.

由此我们得到了一个存在性的结果. 我们或许很难找到这样的一个事件 (而且常常如此), 但是我们知道它存在. 我们在这里给出三个由 Erdős 提出的概率方法的例子 (复杂度逐渐增加), 而以一个特别优雅的最近的应用来结束.

作为热身, 考虑由子集 A_i 组成的一个集族 $\mathcal{F}$, 所有的 A_i 是有限集合 X 上基数为 $d \geqslant 2$ 的子集. 如果存在一种 X 的两种颜色的着色方案, 使得在每一个 A_i 中, 两种颜色都存在, 我们说 $\mathcal{F}$ 是 2-可着色的. 我们立刻就可以推出并不是任何的集族都能如此着色的. 举一个例子, 考虑一个 $(2d-1)$ 元集 X 的所有 d 元子集. 那么无论我们怎样对 X 进行 2-着色, 一定存在 d 个元素的颜色是一样的. 另一方面, 同样清楚的是任何 d 元 2-可着色集族的子集族一定是 2-可着色的. 因此我们感兴趣的是最小的 $m = m(d)$, 使得存在一个 m 个元素的集族不是 2-可着色的. 换句话说, $m(d)$ 是保证任意元素个数小于它的集族都是 2-可着色的最大的数.

定理 1. 任意不超过 2^{d-1} 个 d 元集的集族都是 2-可着色的, 也就是说, $m(d) > 2^{d-1}$.

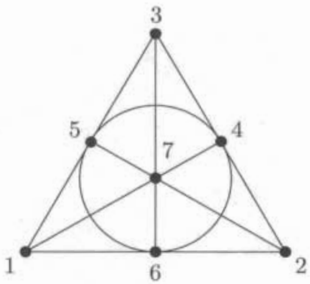
■ **证明.** 假设 $\mathcal{F}$ 是由至多包含 2^{d-1} 个元素的 d 元集组成的集族. 给 X 随机地着两种颜色, 着每种颜色的概率相同. 对每个 $A \in \mathcal{F}$, 令 E_A 表示所有 A 中的元素都是同样的颜色的事件. 因为恰好就有这两种着色, 所以

$$\text{Prob}(E_A) = \left(\tfrac{1}{2}\right)^{d-1},$$

因此由 $m = |\mathcal{F}| \leqslant 2^{d-1}$ 我们得到 (注意到事件E_A是不相交的)

$$\text{Prob}\Big(\bigcup_{A\in\mathcal{F}} E_A\Big) < \sum_{A\in\mathcal{F}} \text{Prob}(E_A) = m\left(\tfrac{1}{2}\right)^{d-1} \leqslant 1.$$

我们得到一定存在某种 X 的 2- 着色方案, 使得没有一个 $\mathcal{F}$ 中的 d 元集是单色的. 这正是我们所说的 2- 可着色性的条件. □

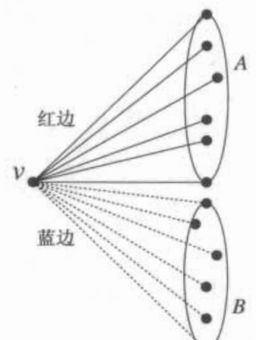


$m(d)$ 的一个上界, 大约等于 $d^2 2^d$, 也被 Erdős 用概率方法得到了, 这一次是通过取随机的集合以及固定一种颜色. 至于准确值, 只有前两个 $m(2) = 3$ 和 $m(3) = 7$ 是已知的. 显然, $m(2) = 3$ 是在图 K_3 上实现的, 而 Fano 构形推出 $m(3) \leqslant 7$. 在这里 $\mathcal{F}$ 是由图上的七个三元集 (包括中间那个圆环集$\{4, 5, 6\}$) 所组成的. 读者可能会饶有兴致地发现 $\mathcal{F}$ 需要三种颜色. 为了证明所有由六个三元集组成的集族是 2- 可着色的, 从而得出 $m(3) = 7$ 我们需要进一步的努力.

我们的下一个例子在这个领域是经典的一个例子 ——Ramsey 数. 考虑在 N 个顶点上的完全图 K_N. 如果无论我们怎样将 K_N 的边着成红色或者蓝色, 总存在一个在 m 个顶点上的完全子图, 其上所有的边都是红的, 或者一个在 n 个顶点上的完全子图, 其上所有的边都是蓝的, 我们说 K_N 具有性质 (m, n). 显然如果 K_N 具有性质 (m, n), 那么对每个 $s \geqslant N$, K_s 都有这个性质. 所以, 就像是在第一个例子中的一样, 我们要求满足这样性质的 N 的最小者 (如果存在的话) —— 这就是 *Ramsey 数* $R(m, n)$.

作为开始, 我们当然有 $R(m, 2) = m$, 因为或者所有 K_m 的边都是红的或者存在一条蓝边, 导致我们得到一个蓝的 K_2. 由对称性, 我们有 $R(2, n) = n$. 现在, 我们假设 $R(m-1, n)$ 和 $R(m, n-1)$ 都存在. 我们然后将要证明 $R(m, n)$ 也存在并且

$$R(m, n) \leqslant R(m-1, n) + R(m, n-1). \tag{1}$$



假设 $N = R(m-1, n) + R(m, n-1)$, 并且考虑任意一个 K_N 的红蓝着色方案. 对某个顶点 v, 令 A 是所有以红边连接 v 的顶点的集合, 而 B 是所有以蓝边连接的顶点的集合.

因为 $|A| + |B| = N - 1$, 我们发现或者 $|A| \geqslant R(m-1, n)$ 或者 $|B| \geqslant R(m, n-1)$. 假设 $|A| \geqslant R(m-1, n)$, 另外的情况类似. 那么由 $R(m-1, n)$ 的定义, 要么存在 A 中元素个数为 $m-1$ 的子集 A_R, 其所有边都着成红色, 与 v 一起组成了一个红色的 K_m, 要么存在元

素个数为 n 的, 所有的边都着成蓝色的子集 A_B. 我们推出 K_N 满足 (m,n) 性质, 并且断言 (1) 成立.

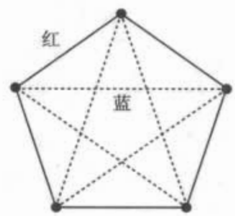
结合 (1) 及初始值 $R(m,2)=m$ 和 $R(2,n)=n$, 我们用类似求得二项式系数的递归法获得

$$R(m,n) \leqslant \binom{m+n-2}{m-1},$$

并且特别地有

$$R(k,k) \leqslant \binom{2k-2}{k-1} = \binom{2k-3}{k-1} + \binom{2k-3}{k-2} \leqslant 2^{2k-3}. \quad (2)$$

现在我们真正感兴趣的是 $R(k,k)$ 的下界. 这相当于证明对一个充分大的 $N<R(k,k)$ 存在一种对边的着色方案使得最后没有红色或蓝色的 K_k. 而这就是概率方法出场的时候了.



定理 2. 对所有的 $k \geqslant 2$, Ramsey 数有如下下界:

$$R(k,k) \geqslant 2^{\frac{k}{2}}.$$

■ **证明.** 我们有 $R(2,2)=2$. 而由 (2) 我们知道 $R(3,3) \leqslant 6$, 而按照如图的方案着色的多边形证明了 $R(3,3)=6$.

现在假定 $k \geqslant 4$. 假设 $N<2^{\frac{k}{2}}$, 考虑所有红蓝着色方案, 其中我们对每一条边独立地等概率地红蓝着色. 这样, 每种着色方案都是同样地以概率 $2^{-\binom{N}{2}}$ 出现. 令 A 是一个有 k 个顶点的集合. 那么 A 中的边都被着成红色的这个事件 A_R 的概率就是 $2^{-\binom{k}{2}}$. 因此我们可以推出某个 k 元集被着成全红色的概率 p_R 被以下的关系式控制住:

$$p_R = \text{Prob}\Big(\bigcup_{|A|=k} A_R\Big) \leqslant \sum_{|A|=k} \text{Prob}(A_R) = \binom{N}{k} 2^{-\binom{k}{2}}.$$

现在利用 $N<2^{\frac{k}{2}}$ 和 $k \geqslant 4$, 再加上 $k \geqslant 2$ 的不等式 $\binom{N}{k} \leqslant \frac{N^k}{2^{k-1}}$ (参见第2章附录), 我们有

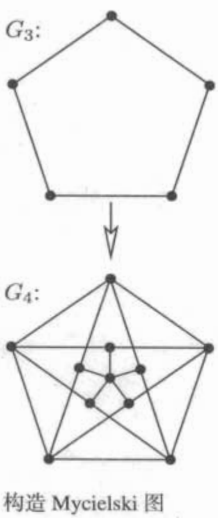
$$\binom{N}{k} 2^{-\binom{k}{2}} \leqslant \frac{N^k}{2^{k-1}} 2^{-\binom{k}{2}} < 2^{\frac{k^2}{2}-\binom{k}{2}-k+1} = 2^{-\frac{k}{2}+1} \leqslant \frac{1}{2}.$$

因此有 $p_R<\frac{1}{2}$, 而由对称性, 某个具有 k 个顶点的集合, 其中每条边都着成蓝色的概率 $p_B<\frac{1}{2}$. 我们可得结论: 对 $N<2^{\frac{k}{2}}$, $p_R+p_B<1$, 所以一定存在一种非红非蓝的着色方案 K_k, 而这说明 K_N 没有性质 (k,k). □

当然, $R(k,k)$ 中的上界和下界有很大的距离. 就像这本证明集一样简单的是, 在 Erdős 的结果出现 50 多年以后, 对一般的 k 仍没有找到更好的下界. 事实上, 没有人能够证明对某个固定的 $\varepsilon > 0$, 有 $R(k,k) > 2^{(\frac{1}{2}+\varepsilon)k}$ 或者 $R(k,k) < 2^{(2-\varepsilon)k}$.

我们的第三个结果是另一个对概率方法的漂亮阐述. 考虑一个在 n 个顶点上的图 G 以及其色数 $\chi(G)$. 如果 $\chi(G)$ 很大, 那也就是说, 我们需要很多的颜色, 那么我们会怀疑是否 G 包含一个大的完全子图. 但是, 远不是这么回事. 早在40年代 Blanche Descartes 就已经构造了有任意大的色数但没有三角形的图, 也就是说, 每一个圈都至少有 4 条边, 其他的也一样 (请参考下面的方框) .

但是, 在这些例子中有很多圈是有四条边的. 我们能做得更好一点吗? 我们能描绘出不存在长度较短的圈而仍旧有很大的色数吗? 我们可以! 为了更精确, 我们将图 G 中的最短圈的长度称为 G 的围长, 记为 $\gamma(G)$; 那么我们就得到以下的定理, 首先为 Paul Erdős 所证明.



构造 Mycielski 图

大色数且无三角形的图

这是一串无三角形的图 $G_3, G_4, \cdots$, 满足

$$\chi(G_n) = n.$$

从 $G_3 = C_5$ 这个五边形开始, 我们得到 $\chi(G_3) = 3$. 假设我们已经在顶点集 V 上构造了 G_n. 而新的图 G_{n+1} 有顶点集 $V \cup V' \cup \{z\}$, 其中顶点 $v' \in V'$ 与 $v \in V$ 一一对应, 而 z 是一个单独的另外的顶点. G_{n+1} 的边可以分成三类: 第一类是G_n 的所有边; 第二类是每一个 v' 与 G_n 中的顶点 v 的邻居连接的边; 第三类是z 与所有 $v' \in V'$ 连接的边. 由 $G_3 = C_5$ 我们得到 G_4, 所谓的 *Mycielski* 图.

显然, G_{n+1} 也是没有三角形的. 为了证明 $\chi(G_{n+1}) = n+1$, 我们对 n 使用归纳法. 对 G_n 的任意一个 n- 着色方案, 考虑一个颜色族 C. 必定存在一个顶点 $v \in C$, 它与每一个其他颜色的类中的至少一个顶点是相连的; 否则我们可以将 C 中的顶点分配到 $n-1$ 个其他的颜色类当中, 结果出现 $\chi(G_n) \leqslant n-1$. 但现在很明显的是 v' (V' 中的与 v 对应的顶点) 必须在 n- 着色方案中与 v 有相同的颜色. 所以所有的 n 种颜色在 V' 中均出现, 而我们需要一种新颜色来为 z着色.

定理 3. 对于每个 $k \geqslant 2$, 存在一个图 G 满足色数 $\chi(G) > k$ 以及围长 $\gamma(G) > k$.

证明的策略与前面的那些证明类似: 我们考虑一个特定的图上的概率空间, 并且证明 $\chi(G) \leqslant k$ 的概率小于 $\frac{1}{2}$ 即可, 而同样地 $\gamma(G) \leqslant k$ 的概率小于 $\frac{1}{2}$. 结果, 我们想要的特定性质的图一定是存在的.

■ **证明.** 令 $V = \{v_1, v_2, \cdots, v_n\}$ 是顶点集, 而 p 是一个将要精心挑选的 0 到 1 之间的固定的数. 我们的概率空间 $\mathcal{G}(n,p)$ 由所有在 V 上的, 单个的边以概率 p 独立出现的图所组成的. 换句话说, 我们在谈论的是一个 Bernoulli 实验, 我们在每一条边上赋予的概率为 p. 作为例子, 一个完全图的概率 $\text{Prob}(K_n)$ 是 $\text{Prob}(K_n) = p^{\binom{n}{2}}$. 一般地, 我们有 $\text{Prob}(H) = p^m(1-p)^{\binom{n}{2}-m}$, 如果在 V 上的图 H 恰好有 m 条边.

让我们首先来看看色数 $\chi(G)$. 我们用 $\alpha = \alpha(G)$ 表示*独立数*, 也就是 G 中最大的独立集的顶点个数. 因为在一种 $\chi = \chi(G)$ 的着色方案当中所有的着色类都是独立的 (而因此基数 $\leqslant \alpha$), 我们推断得 $\chi(\alpha) \geqslant n$. 因此如果 α 相对于 n 比较小的话, χ 一定是比较大的, 而这就是我们想要的.

假设 $2 \leqslant r \leqslant n$. 某个固定的 V 中的 r 元集是独立的概率为 $(1-p)^{\binom{r}{2}}$, 并且由与定理 2 同样的论证以及对所有的 p 有 $1-p \leqslant$

e^{-p}, 我们可得

$$\begin{aligned}\text{Prob}(\alpha \geqslant r) &\leqslant \binom{n}{r}(1-p)^{\binom{r}{2}}\\ &\leqslant n^r(1-p)^{\binom{r}{2}} = (n(1-p)^{\frac{r-1}{2}})^r \leqslant (ne^{-p(r-1)/2})^r,\end{aligned}$$

给定某一个固定的 $k > 0$, 我们现在选择 $p := n^{-\frac{k}{k+1}}$, 并继续证明对充分大的 n,

$$\text{Prob}\Big(\alpha \geqslant \frac{n}{2k}\Big) < \frac{1}{2}. \tag{3}$$

事实上, 因为 $n^{\frac{1}{k+1}}$ 比 $\log n$ 增长要快, 对充分大的 n 我们有 $n^{\frac{1}{k+1}} \geqslant 6k\log n$, 因此 $p \geqslant 6k\frac{\log n}{n}$. 对 $r := \lceil \frac{n}{2k} \rceil$ 这能推出 $pr \geqslant 3\log n$, 而由此

$$ne^{-p(r-1)/2} = ne^{-\frac{pr}{2}}e^{\frac{p}{2}} \leqslant ne^{-\frac{3}{2}\log n}e^{\frac{1}{2}} = n^{-\frac{1}{2}}e^{\frac{1}{2}} = (\tfrac{e}{n})^{\frac{1}{2}},$$

当 n 趋向于正无穷的时候收敛到 0. 因此 (3) 对所有 $n \geqslant n_1$ 均成立.

现在我们看看第二个参数$\gamma(G)$. 对一个给定的 k 我们想要证明没有很多的长度 $\leqslant k$ 的圈. 令 i 为一个在 3 和 k 之间的数, 而 $A \subseteq V$ 是一个固定的 i 元集. 所有可能的 A 上的 i 边形的圈的个数显然就是 A 上的循环置换的数目除以 2 (因为我们能从两个不同的方向置换一个圈), 而因此等于 $\frac{(i-1)!}{2}$. 从而所有可能的 i 边形的圈的个数就是 $\binom{n}{i}\frac{(i-1)!}{2}$, 因此每一个这样的圈 C 都以概率 p^i 出现. 令 X 为记录长度 $\leqslant k$ 的圈的个数的随机变量. 为了估计 X 我们运用两个简单但是漂亮的工具. 第一个是期望的线性性, 而第二个是非负随机变量的 Markov 不等式,即

$$\text{Prob}(X \geqslant a) \leqslant \frac{EX}{a},$$

其中 EX 是 X 的期望. 关于这两个工具请参考第 14 章的附录.

令 X_C 是一个长度为 i 的圈 C 的指示随机变量. 也就是说, $X_C = 1$ 还是 0 取决于 C 是否出现在图中, 因此 $EX_C = p^i$. 因为 X 记录了所有长度 $\leqslant k$ 的圈的个数, 我们有 $X = \sum X_C$, 而由线性性可知

$$EX = \sum_{i=3}^{k}\binom{n}{i}\frac{(i-1)!}{2}p^i \leqslant \frac{1}{2}\sum_{i=3}^{k}n^ip^i \leqslant \frac{1}{2}(k-2)n^kp^k,$$

其中最后一个不等式成立是因为 $np = n^{\frac{1}{k+1}} \geqslant 1$. 现在运用 Markov 不等式, 取 $a = \frac{n}{2}$, 我们得到

$$\text{Prob}(X \geqslant \tfrac{n}{2}) \leqslant \frac{EX}{n/2} \leqslant (k-2)\frac{(np)^k}{n} = (k-2)n^{-\frac{1}{k+1}}.$$

因为右端在 n 趋向于正无穷的时候收敛于 0, 我们推断得对 $n \geqslant n_2$, $p(X \geqslant \frac{n}{2}) < \frac{1}{2}$.

现在我们差不多完成了. 我们的分析告诉我们对 $n \geqslant \max(n_1, n_2)$, 存在 n 个顶点上的图 H 满足 $\alpha(H) < \frac{n}{2k}$, 并且具有少于 $\frac{n}{2}$ 个长度 $\leqslant k$ 的圈. 从每一个这样的圈中删掉一个顶点, 而令 G 为剩下的图. 那么 $\gamma(G) > k$ 在任意的比率下都成立. 因为 G 包含多于 $\frac{n}{2}$ 个顶点并且满足 $\alpha(G) \leqslant \alpha(H) < \frac{n}{2k}$, 我们发现

$$\chi(G) \geqslant \frac{n/2}{\alpha(G)} \geqslant \frac{n}{2\alpha(H)} > \frac{n}{n/k} = k,$$

证毕. □

对于数值较大的围长和色数的 (庞大的) 图的明确构造方法我们是知道的. (相反, 我们不知道怎样构造红/蓝着色方案, 使得里面没有大的单色团, 而这种着色方案的存在性是由定理 2 所保证了的.) Erdős 的证明中剩下的激动人心的部分是它证明了相对比较小的色数和围长的数值较大图的存在.

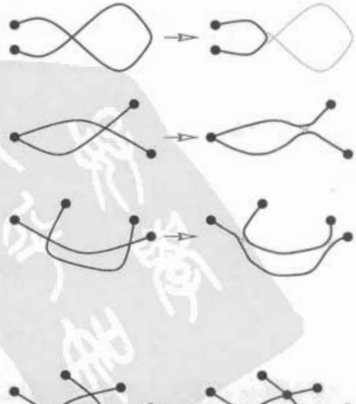
为了结束我们这次到概率世界的短途旅行, 让我们讨论一个在几何图论当中的重要结果 (同样地我们回到 Paul Erdős 身上) .

考虑一个有 n 个顶点和 m 条边的简单图 $G = G(V, E)$. 我们想要将 G 嵌入一个平面, 就像我们对平面图做的那样. 现在, 我们从第 11 章可以知道 —— 作为 Euler 公式的结果 —— 一个简单的平面图 G 最多有 $3n - 6$ 条边. 因此, 如果 m 比 $3n - 6$ 大, 那么一定有交叉的边存在. *交叉数* $\mathrm{cr}(G)$ 就被这样自然地定义了: 它是在 G 的所有画法中交叉的最小数目, 其中多于两条的边交于一个顶点的交叉是不被允许的. 因此 $\mathrm{cr}(G) = 0$ 当且仅当 G 是平面图.

在这样的最小图中以下三种情况被排除了:

- 没有边能自交
- 有共同端点的边不能相交.
- 没有两条边能相交两次.

这是因为在任意的一个情况当中, 我们可以构造同一个与该图不同的图, 但是具有更少的交叉, 运用我们在图中表示的操作. 所以, 从现在起我们假定所有的画法都有这三条规则.



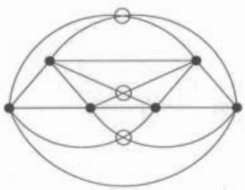
假定 G 被画在平面上, 其交叉数为 $\mathrm{cr}(G)$. 我们可以立刻推断出交叉数的一个下界. 考虑以下的图 H: H 的顶点是 G 的顶点加上所有的交叉点, 而所有的边是原来的边的部分, 即我们沿着交叉点到交叉点.

新图 H 现在就是简单平面图 (这可以由我们的三个假定得到!). H 的顶点数是 $n+\mathrm{cr}(G)$ 而边数为 $m+2\mathrm{cr}(G)$, 因为每个交叉处的新顶点都是 4 度. 对于平面图的边的个数的界我们发现:

$$m+2\,\mathrm{cr}(G) \;\leqslant\; 3(n+\mathrm{cr}(G))-6,$$

即,

$$\mathrm{cr}(G) \;\geqslant\; m-3n+6. \tag{4}$$



作为一个例子, 对完全图 K_6 我们计算

$$\mathrm{cr}(K_6) \geqslant 15-18+6=3,$$

并且事实上存在一个画法只有三个交叉.

(4) 中的下界对于 m 关于 n 是线性的情况下来看是足够好的, 然后图画变了, 而这就是我们的定理.

定理 4. *令 G 是具有 n 个顶点和 m 条边的简单图, 其中 $m \geqslant 4n$. 那么*

$$\mathrm{cr}(G) \;\geqslant\; \frac{1}{64}\frac{m^3}{n^2}.$$

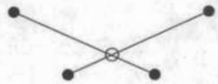
这个被称作*交叉引理*的结果的历史, 是非常有趣的. 在 1973 年 Erdős 和 Guy 提出这个猜想 (其中 $\frac{1}{64}$ 是被一个常数 c 所取代的). 最初的证明是由 Leighton 在 1982 年给出的 (用 $\frac{1}{100}$ 代替 $\frac{1}{64}$), 而另外又由 Ajtai, Chvátal, Newborn 和 Szemerédi 独立地得到. 交叉引理几乎不为人所知 (事实上, 许多人在它的原始证明出来很久以后仍然认为这是一个猜想), 直到 László Székely 在他的一篇很漂亮的论文里面将其运用到一系列至那时为止都是相当困难的几何极植问题上, 阐述了其有用性. 以下我们要提供的证明是从 Bernard Chazelle, Micha Sharir 和 Emo Welzl 的电子邮件谈话里提炼出来的, 毫无疑问这应该属于数学天书.

■ **证明.** 考虑 G 的最小化画图, 且令 p 是一个 0 到 1 之间的数 (将会在以后确定). 现在我们产生 G 的一个子图, 选取 G 中的顶点以概率 p 落入这个子图, 相互独立. 我们用 G_p 标记所得到的诱导子图.

令 n_p, m_p, X_p 为对顶点数、边数和 G_p 中的交叉的数目计数的随机变量. 因为由 (4), $\mathrm{cr}(G)-m+3n \geqslant 0$ 对任意的图都成立, 我们当然有

$$E(X_p-m_p+3n_p) \;\geqslant\; 0.$$

现在我们继续来计算单个的期望 $E(n_p)$, $E(m_p)$ 和 $E(X_p)$. 很明显地, $E(n_p) = pn$ 以及 $E(m_p) = p^2m$, 因为一条边出现在 G_p 中当且仅当其两个端点也出现在 G_p 中. 最后, $E(X_p) = p^4\mathrm{cr}(G)$, 因为一个交叉点在 G_p 中出现当且仅当全部四个 (不同的 !) 顶点都在那里.



由期望的线性性我们发现

$$0 \leqslant E(X_p) - E(m_p) + 3E(n_p) = p^4\mathrm{cr}(G) - p^2m + 3pn,$$

也就是

$$\mathrm{cr}(G) \geqslant \frac{p^2m - 3pn}{p^4} = \frac{m}{p^2} - \frac{3n}{p^3}. \tag{5}$$

现在这是最关键的一条: 令 $p := \frac{4n}{m}$ (由我们的假设这至多是 1), 那么 (5) 变成

$$\mathrm{cr}(G) \geqslant \frac{1}{64}\left[\frac{4m}{(n/m)^2} - \frac{3n}{(n/m)^3}\right] = \frac{1}{64}\frac{m^3}{n^2},$$

这就是我们想要的了. □

Paul Erdős 看到这个证明会很高兴的.

参考文献

[1] M. Ajtai, V. Chvátal, M. Newborn & E. Szemerédi: *Crossing-free subgraphs,* Annals of Discrete Math. **12** (1982), 9-12.

[2] N. Alon & J. Spencer: *The Probabilistic Method,* Second edition, Wiley-Interscience 2000.

[3] P. Erdős: *Some remarks on the theory of graphs,* Bulletin. Amer. Math. Soc. **53** (1947), 292-294.

[4] P. Erdős: *Graph theory and probability,* Canadian J. Math. **11** (1959), 34-38.

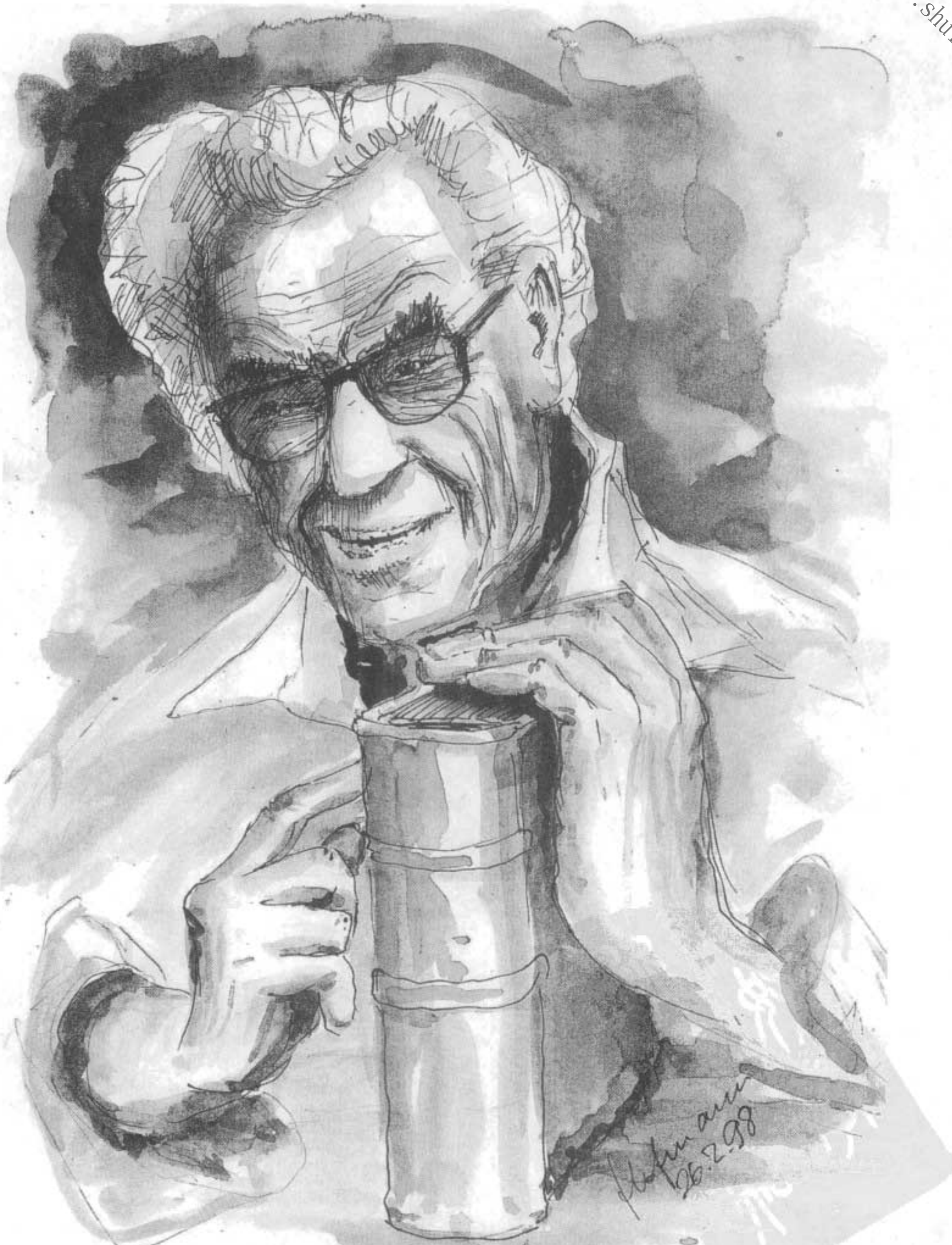
[5] P. Erdős: *On a combinatorial problem I,* Nordisk Math. Tidskrift **11** (1963), 5-10.

[6] P. Erdős & R. K. Guy: *Crossing number problems,* Amer. Math. Monthly **80** (1973), 52-58.

[7] P. Erdős & A. Rényi: *On the evolution of random graphs,* Magyar Tud. Akad. Mat. Kut. Int. Közl. **5** (1960), 17-61.

[8] T. Leighton: *Complexity Issues in VLSI,* MIT Press, Cambridge MA 1983.

[9] L. A. Székely: *Crossing numbers and hard Erdős problems in discrete geometry*, Combinatorics, Probability, and Computing **6** (1997), 353-358.


26.2.98

关于插图的说明

我们很荣幸得到 Karl Heinrich Hofmann (Darmstadt) 的特别许可，能用他的一些漂亮的原创画来装饰本书.

第 11 章的正规多面体的插图和第 12 章末的插图是 WAF Ruppert (维也纳) 提供的.

第 11 章 Sylvester-Gallai 定理中的两个插图是由 Jürgen Richter-Gebert 提供的.

第 31 章中的照片是坐落在 Minneapolis 市的, 由 Frank Gehry 设计的 Weisman 艺术博物馆的西侧正面照片, 由 Chris Faust 提供. 照片右边是位于博物馆西侧后面的 Dolly Fiterman Riverview 艺术画廊的平面设计图.

书中 Bertrand, Cantor, Erdős, Euler, Fermat, Herglotz, Hermite, Hilbert, Pólya, Littlewood 和 Sylvester 的照片来自 Oberwolfach 数学研究所的照片档案, 并得到许可. (非常感谢Annette Disch!)

书中具有 Buffon, Chebyshev, Euler 和 Ramanujan 肖像的邮票来自 Jeff Miller 的数学邮票网址 http://jeff560.tripod.com, 并得到他慷慨的许可.

Hermite 的照片来自他的全集第一卷.

Claude Shannon 的照片是由 MIT 博物馆提供的, 并在获得许可后复制.

Cayley 的肖像取自 "Weierstrass 影集" (Reinhard Bölling 编, Vieweg, 1994), 并得到柏林国家博物馆的现代图书馆许可.

Cauchy 的肖像是从巴黎综合理工学院 (École Polytechnique, Paris) 的收藏中经许可复制的.

Fermat 的照片是从 Stefan Hildebrandt 和 Anthony Tromba 的著作 The Parsimonious Universe, Shape and Form in the Natural World (Springer-Verlag, 1996) 中复制的.

Ernst Witt 的肖像来自 Journal für die Reine und Angewandte Mathematik, 426 (1992), 经 Walter de Gruyter 出版公司许可.

Karol Borsuk 的照片是由 Isaac Namioka 于 1967 年拍摄的, 经同意复制.

Peter Sperner (Braunschweig) 提供了他父亲的肖像, Vera Sós 提供了 Paul Turán 的照片.

Noga Alon 提供了 A. Nilli 的肖像.

在此, 我们一并致谢!

名词索引(数字表示名词出现的章号)